NAVAL POSTGRADUATE SCHOOL

MONTEREY, CALIFORNIA

THESIS

SHADOWS OF STUXNET: RECOMMENDATIONS FOR U.S. POLICY ON CRITICAL INFRASTRUCTURE CYBER DEFENSE DERIVED FROM THE STUXNET ATTACK

by

Ronald L. Lendvay

March 2016

Thesis Co-Advisors: Kathleen Kiernan
John Rollins

Approved for public release; distribution is unlimited

THIS PAGE INTENTIONALLY LEFT BLANK

REPORT DOCUMENTATION PAGE			Form Approved OMB No. 0704–0188
Public reporting burden for this collection of information is estimated to average 1 hour per response, including the time for reviewing instruction, searching existing data sources, gathering and maintaining the data needed, and completing and reviewing the collection of information. Send comments regarding this burden estimate or any other aspect of this collection of information, including suggestions for reducing this burden, to Washington headquarters Services, Directorate for Information Operations and Reports, 1215 Jefferson Davis Highway, Suite 1204, Arlington, VA 22202-4302, and to the Office of Management and Budget, Paperwork Reduction Project (0704-0188) Washington, DC 20503.			
1. AGENCY USE ONLY *(Leave blank)*	**2. REPORT DATE** March 2016	**3. REPORT TYPE AND DATES COVERED** Master's thesis	
4. TITLE AND SUBTITLE SHADOWS OF STUXNET: RECOMMENDATIONS FOR U.S. POLICY ON CRITICAL INFRASTRUCTURE CYBER DEFENSE DERIVED FROM THE STUXNET ATTACK			**5. FUNDING NUMBERS**
6. AUTHOR(S) Ronald L. Lendvay			
7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES) Naval Postgraduate School Monterey, CA 93943-5000			**8. PERFORMING ORGANIZATION REPORT NUMBER**
9. SPONSORING /MONITORING AGENCY NAME(S) AND ADDRESS(ES) N/A			**10. SPONSORING / MONITORING AGENCY REPORT NUMBER**
11. SUPPLEMENTARY NOTES The views expressed in this thesis are those of the author and do not reflect the official policy or position of the Department of Defense or the U.S. Government. IRB Protocol number ____N/A____.			
12a. DISTRIBUTION / AVAILABILITY STATEMENT Approved for public release; distribution is unlimited			**12b. DISTRIBUTION CODE** A

13. ABSTRACT (maximum 200 words)

In June 2012, the worldwide cyber security landscape changed when the presence of a new and sophisticated malware, later dubbed "Stuxnet," was discovered in the computers of an Iranian nuclear facility. The malware was a cyber weapon, programmed to destroy the industrial machinery utilized for uranium enrichment. Stuxnet was soon dissected and diagnosed as a pioneering and politically motivated cyber attack that successfully infiltrated a high-security, government-run critical infrastructure and destroyed its physical property with computer code. The potential consequences of a similar attack on vulnerable U.S. critical infrastructures could be devastating.

This thesis begins with a review of the evolution of U.S. policy related to the cyber defense of critical infrastructures. It then examines the critical infrastructure sectors within the United States, its dependency on computer technology, and the potential consequences of cyber attacks. A detailed case study of the Stuxnet attack follows, along with an analysis of the lessons learned from Stuxnet.

The thesis concludes with specific policy improvement recommendations for the United States under three major themes: enhancing national unity of effort, expansion of cyber security coordination between the private and government sectors, and incentivizing private-sector compliance with best practices in cyber security.

14. SUBJECT TERMS Cyber Emergency Response Team (CERT), critical infrastructure (CI), cyber security, distributed control systems (DCS), distributed denial of service (DDoS), executive order (EO), industrial control systems (ICS), information technology (IT), National Institute of Standards and Technology (NIST), presidential decision directive (PDD), Programmable Logic Controller (PLC), Supervisory Control and Data Acquisition (SCADA)			**15. NUMBER OF PAGES** 137 / **16. PRICE CODE**
17. SECURITY CLASSIFICATION OF REPORT Unclassified	**18. SECURITY CLASSIFICATION OF THIS PAGE** Unclassified	**19. SECURITY CLASSIFICATION OF ABSTRACT** Unclassified	**20. LIMITATION OF ABSTRACT** UU

THIS PAGE INTENTIONALLY LEFT BLANK

Approved for public release; distribution is unlimited

SHADOWS OF STUXNET: RECOMMENDATIONS FOR U.S. POLICY ON CRITICAL INFRASTRUCTURE CYBER DEFENSE DERIVED FROM THE STUXNET ATTACK

Ronald L. Lendvay
Chief of Homeland Security, Jacksonville Sheriff's Office, Florida
B.A., University of North Florida, 1991

Submitted in partial fulfillment of the
requirements for the degree of

**MASTER OF ARTS IN SECURITY STUDIES
(HOMELAND SECURITY AND DEFENSE)**

from the

**NAVAL POSTGRADUATE SCHOOL
March 2016**

Approved by: Kathleen Kiernan
Thesis Co-Advisor

John Rollins
Thesis Co-Advisor

Erik Dahl
Associate Chair of Instruction
Department of National Security Affairs

THIS PAGE INTENTIONALLY LEFT BLANK

ABSTRACT

In June 2012, the worldwide cyber security landscape changed when the presence of a new and sophisticated malware, later dubbed “Stuxnet,” was discovered in the computers of an Iranian nuclear facility. The malware was a cyber weapon, programmed to destroy the industrial machinery utilized for uranium enrichment. Stuxnet was soon dissected and diagnosed as a pioneering and politically motivated cyber attack that successfully infiltrated a high-security, government-run critical infrastructure and destroyed its physical property with computer code. The potential consequences of a similar attack on vulnerable U.S. critical infrastructures could be devastating.

This thesis begins with a review of the evolution of U.S. policy related to the cyber defense of critical infrastructures. It then examines the critical infrastructure sectors within the United States, its dependency on computer technology, and the potential consequences of cyber attacks. A detailed case study of the Stuxnet attack follows, along with an analysis of the lessons learned from Stuxnet.

The thesis concludes with specific policy improvement recommendations for the United States under three major themes: enhancing national unity of effort, expansion of cyber security coordination between the private and government sectors, and incentivizing private-sector compliance with best practices in cyber security.

THIS PAGE INTENTIONALLY LEFT BLANK

TABLE OF CONTENTS

LIST OF FIGURES

THIS PAGE INTENTIONALLY LEFT BLANK

LIST OF TABLES

THIS PAGE INTENTIONALLY LEFT BLANK

LIST OF ACRONYMS AND ABBREVIATIONS

ACSC	Australian Cyber Security Centre
CD	compact disc
CERT	Cyber Emergency Response Team
CHDS	Center for Homeland Defense and Security
CI	critical infrastructure
CIA	Central Intelligence Agency
CISP	Cybersecurity Information Sharing Partnership
CNCI	Comprehensive National Cybersecurity Initiative
CRS	Congressional Research Service
DCS	distributed control systems
DDoS	distributed Denial of Service
DOD	Department of Defense
DOE	Department of Energy
DHS	Department of Homeland Security
DVD	digital versatile disc
EO	Executive Order
FBI	Federal Bureau of Investigation
FDNY	Fire Department of New York
GAO	Government Accountability Office
IAEA	International Atomic Energy Agency
ICS	industrial control systems
ICS-CERT	Industrial Control Systems Cyber Emergency Response Team
IEEE	Institute of Electrical and Electronics Engineers
IT	information technology
NIPP	National Infrastructure Protection Plan
NIST	National Institute of Standards and Technology
NPS	Naval Postgraduate School
NPT	Nuclear Nonproliferation Treaty
NSA	National Security Agency
NYPD	New York Police Department
OPM	Office of Personnel Management

PDD	presidential decision directive
PPD 21	Presidential Policy Directive 21
PLC	programmable logic controller
SCADA	supervisory control and data acquisition
SLTT	state, local, territorial and tribal governments
SSA	sector specific agency
STEM	science, technology, engineering and mathematics
TISN	trusted information sharing network
UN	United Nations
U.K.	United Kingdom
U.S.	United States
USB	universal serial bus
USCYBERCOM	United States Cyber Command

EXECUTIVE SUMMARY

Cyber security for critical infrastructures (CIs) ranks among the highest U.S. national security priorities. The national well-being and the fabric of American's daily lives rely upon the security and resiliency of CIs. The Department of Homeland Security (DHS) refers to (CI) as the, "backbone of our nation's economy, security and health."[1] While Americans may not think about it, they unknowingly interact with CI in their daily lives through the electricity used and the clean water consumed. Computerized CIs also affect everyone's daily lives by managing the transportation systems used for personal or business travel and the communications systems utilized to stay connected with friends, family, and coworkers.[2] Interruptions to these or other critical services, such as delivering public safety and national defense, could be disruptive or devastating for this nation's well-being and security. The CI systems and facilities that provide these foundational services have become increasingly computer reliant and networked. Computerized components, called industrial control systems (ICS), measure and control many of the industrial or mechanical processes needed to produce the desired outputs of U.S. CIs.

This thesis identifies the pivotal areas of U.S. CI cyber security policy that could be enhanced to provide the most effective overarching solutions to the current vulnerabilities highlighted by the Stuxnet attack on Iran's Natanz Uranium enrichment facility. The Stuxnet attack is the first publicly known use of a cyber-weapon to destroy the CI of another country, accomplishing with computer programming, what only used to be possible through bombing or traditional sabotage.[3] It provides a blueprint for how to conduct a specifically targeted cyber

[1] "What Is Critical Infrastructure?," last modified October 24, 2013, http://www.dhs.gov/what-critical-infrastructure.

[2] Ibid.

[3] David Sanger, "Obama Order Sped Up Wave of Cyberattacks Against Iran," *New York Times*, May 31, 2012, http://www.nytimes.com/2012/06/01/world/middleeast/obama-ordered-wave-of-cyberattacks-against-iran.html?pagewanted=all&_r=0.

attack on the computer systems of a high security government controlled CI target.[4] More specifically, it shows potential cyber adversaries how to inject malicious code into real time ICS controllers.[5]

Three crucial points of failure contributed to the vulnerability that allowed Stuxnet to infiltrate, thrive within, and destroy centrifuges at Natanz. The first point of failure at Natanz, leading to the Stuxnet infection, was the insider threat of system access at the facility. Stuxnet was engineered to be hand carried into the Natanz plant to infect the computer network. The second point of failure at Natanz was the successful spread of Stuxnet through the air-gapped network to the programmable logic controllers (PLC), which controlled the precise spinning speed needed for proper centrifuge operations. These first two points of failure fall underneath the third point of failure, which was a deficiency in cyber security policy. Although the Iranian government will not publicly share its Natanz policy portfolio, a deficiency occurred in either establishing or following appropriate security protocols that led to the system access and system security breakdowns noted as the first two points of failure.

Three key areas where policy enhancement could bolster U.S. national CI and ICS defenses have been identified as: enhancing national unity of effort, expansion of the coordination of effort between the private and government sectors, and incentivizing private sector compliance with best practices in cyber security.

Three corresponding policy recommendations derived from these key areas for enhancement include:

- The creation of a new federal Department of Cyber Affairs, led by a presidential cabinet level Secretary of Cyber Affairs, and the

[4] Stamatis Karnouskos, "Stuxnet Worm Impact on Industrial Cyber-Physical System Security," paper presented at the 37th Annual Conference of the IEEE Industrial Electronics Society (IECON 2011), Melbourne, Australia, November 7–10, 2011, http://papers.duckdns.org/files/2011_IECON_stuxnet.pdf.

[5] Ralph Langer, "To Kill a Centrifuge," The Langer Group, November 2013, 19, http://www.langner.com/en/wp-content/uploads/2013/11/To-kill-a-centrifuge.pdf.

subsequent assignment to the department of developing a unified cyber security policy for the United States.

- The consolidation of U.S. government cyber security expertise and assets for a more focused approach toward unified cyber defense for U.S. CIs.
- The development of a voluntary business cyber security certification program that allows businesses exhibiting cyber security best practices to be recognized in the marketplace for their commitment by customers, investors and partners similar to the United Kingdom's (U.K.'s) "Cyber Essentials" program.

These recommendations would most effectively be implemented together as programs managed under a new federal Department of Cyber Affairs. The second two recommendations could also potentially be implemented independently and managed by separate government entities, which could be assigned responsibility for the separate recommendations. The disadvantage to that approach would be the continued fragmentation of cyber security responsibility among stakeholders within the United States when unity of effort should be the key to this diverse landscape of military, government, business and private sectors owners of U.S. CI.

THIS PAGE INTENTIONALLY LEFT BLANK

ACKNOWLEDGMENTS

Participating in the Center for Homeland Defense and Security (CHDS) educational experience at the Naval Postgraduate School has been both an honor and a privilege. Standing with my classmates from the Fire Department of New York and New York Police Department during the base's 09/11 memorial service, during our very first in-residence session, was an experience that fortified my decision to take on this challenge. The Department of Homeland Security deserves accolades for developing and funding this first-rate educational experience for homeland security professionals.

I am grateful for the support of the outstanding CHDS staff and faculty who were committed to making this program a rewarding experience. I also must acknowledge my classmates, who added greatly to the learning experience, and were an outstanding group with whom to share this experience. I was fortunate to have the dedicated support of my thesis advisors, Kathleen Kiernan and John Rollins, who provided the guidance necessary to complete this thesis successfully.

My participation in this program would not have been possible without the support of the Jacksonville Sheriff's Office. Sheriff John Rutherford's authorization of my attendance, and Sheriff Mike Williams' encouragement to apply, speaks volumes about their commitment to serve the Jacksonville community with the most educated and distinguished homeland security professionals possible. I am thankful for my co-workers who covered my obligations at the office while I traveled for in-residence school sessions.

Most importantly, I am blessed to have the unwavering support of my wonderful wife, Lisa, and our two beautiful daughters, Sarah and Audrey. They all sacrificed quality time with me while selflessly sharing me with my work and school responsibilities. I appreciate the love and encouragement provided by my parents, Ron and Kathy, who have encouraged me throughout my life. Without

the love and support of my family, neither this thesis nor this educational experience would have been possible. For this, I am eternally grateful.

I. INTRODUCTION

U.S. critical infrastructure (CI) facilities rely on computer hardware and software systems to control and monitor their industrial processes.[1] These computer systems are referred to as industrial control systems (ICS). The National Institute of Standards and Technology (NIST) defines ICS as "combinations of control components that act together to achieve an industrial objective."[2] NIST further relates that ICS are "critical to the operation of U.S. CIs" and regulate the industrial processes commonly found in the "electrical, water and wastewater, oil and natural gas, chemical, transportation, pharmaceutical, pulp and paper, food and beverage, and discrete manufacturing (e.g., automotive, aerospace, and durable goods) industries."[3]

A. PROBLEM STATEMENT

Early deployments of ICS in this country were initially viewed as being vulnerable to only local threats because their components were often part of stand-alone systems not connected to networks. Primary threats were thwarted with physical barriers for equipment and focused on screening personnel with access to the system. The threat landscape has drastically changed with modern networking trends toward integrating CI ICS with company information technology (IT) and wireless networks.[4]

Threats to this nation's CIs can come from a variety of sources to include hostile governments, terrorist groups, industrial spies, organized crime groups,

[1] Paul K. Kerr, John Rollins, and Catherine A. Theohary, *The Stuxnet Computer Worm: Harbinger of an Emerging Warfare Capability* (CRS Report No. R41524) (Washington, DC: Congressional Research Service, 2010), http://www.fas.org/sgp/crs/natsec/R41524.pdf.

[2] Keith Stouffer et al., *Guide to Industrial Control Systems Security* (NIST-800-82) (Gaithersburg, MD: National Institute of Standards and Technology, 2014), 2–1, http://csrc.nist.gov/publications/nistpubs/800-82/SP800-82-final.pdf.

[3] Ibid.

[4] Ibid.

computer hackers, disgruntled employees, and malicious intruders.[5] A crippling malware attack to CI, in almost any of the above noted sectors, could be economically devastating and could even lead to the loss of lives. Disruptions in service could affect this country's government's ability to provide basic domestic or international security services, create gaps in essential public sector services for lengthy periods of time, and foster a loss of public confidence in government.[6]

Vulnerabilities in CI ICS, and their computer networks, have been highlighted by the 2010 discovery of the Stuxnet worm. The sophisticated malware attack carries serious implications for ICS common in CIs throughout the world and in the United States.[7] Stuxnet is the first publicly recognized example of a cyber-weapon being used to attack and destroy industrial machinery.[8] The Stuxnet worm was unprecedented because it was programmed to penetrate and attack ICS specifically, used by CI facilities, and cause long-term damage or destruction to them.[9] The Stuxnet code is currently available in the public domain of the Internet for tailoring and target customization.[10]

The technical vulnerabilities of CI computer systems have been a topic of increasing concern for government, technology and computer security experts. The objective of this thesis is to identify the pivotal areas of U.S. CI cyber protection policy that could be enhanced to provide the most effective overarching solutions to the current vulnerabilities highlighted by the Stuxnet attack on Iran, and provide subsequent recommendations for policy

[5] "Industrial Control Systems Cyber Emergency Response Team," accessed February 13, 2015, https://ics-cert.us-cert.gov/content/cyber-threat-source-descriptions.

[6] Kerr, Rollins, and Theohary, *The Stuxnet Computer Worm*, 7.

[7] Stamatis Karnouskos, "Stuxnet Worm Impact on Industrial Cyber-Physical System Security," paper presented at the 37th Annual Conference of the IEEE Industrial Electronics Society (IECON 2011), Melbourne, Australia, November 7–10, 2011, 4490–4494, http://papers.duckdns.org/files/2011_IECON_stuxnet.pdf.

[8] Jim Finkle, "Researchers Say Stuxnet Was Deployed against Iran in 2007," *Reuters*, February 26, 2013, http://www.reuters.com/article/2013/02/26/us-cyberwar-stuxnet-idUSBRE91P0PP20130226.

[9] Kerr, Rollins, and Theohary, *The Stuxnet Computer Worm*, 6.

[10] Karnouskos, *Stuxnet Worm Impact on Industrial Cyber-Physical System Security*, 4490–4494.

advancements. To arrive at these recommendations, this thesis examines the Stuxnet attack, the vulnerabilities it exploited, and the lessons that may be taken away and applied to U.S. CIs. This thesis does not enter into the political debate or speculation attributing responsibility for launching this attack.

This thesis provides a unique opportunity to study the use of a cyber weapon to target CI, in an unclassified environment, for the benefit of homeland security professionals from all disciplines. Most such attacks are classified and shrouded in secrecy to the point that little information is publicly available. Once current U.S. cyber defense policy for CIs is evaluated, and Stuxnet attack specifics are paired with a foundational understanding of the computerized components within CIs, policy recommendations may be drawn for strengthening overall cyber defense of U.S. CIs.

B. RESEARCH QUESTIONS

The cyber landscape changed when the presence of a new and sophisticated malware, later dubbed Stuxnet, was found in the computers of an Iranian nuclear facility. The code was programmed to control and destroy discreetly the centrifuge components of the Natanz uranium enrichment plant.[11] The Stuxnet worm became the first publicly known use of a cyber-weapon to destroy the CI of another country, accomplishing with computer programming, what only used to be possible through bombing or traditional sabotage.[12]

1. Primary Research Question

What are the policy ramifications that may be drawn from the Stuxnet attack, for industrialized nations, such as the United States that make extensive use of computerized industrial control systems within its CIs?

---

[11] Joby Warrick, "Iran's Natanz Nuclear Facility Recovered Quickly from Stuxnet Cyberattack," *Washington Post*, February 16, 2011, http://www.washingtonpost.com/wp-dyn/content/article/2011/02/15/AR2011021505395.html.

[12] Ellen Nakashima, "Stuxnet Malware Is Blueprint for Computer Attacks on U.S.," *Washington Post*, October 2, 2010, http://www.washingtonpost.com/wp-dyn/content/article/2010/10/01/AR2010100106981.html?sid=ST2010112903583.

2. Ancillary Research Question

What vulnerabilities were exploited within the closed system, high security, CI environment of the Natanz nuclear facility during the Stuxnet attack?

C. RESEARCH DESIGN AND METHODOLOGY

1. Exploratory Case Study

The object of study is the deployment of the Stuxnet malware as an offensive cyber weapon against Iran's Natanz nuclear facility. Stuxnet was the first high profile politically motivated cyber attack[13] that caused significant physical damage to a CI facility.[14] The research method design of this thesis project is that of an exploratory case study of the deployment of the Stuxnet malware. At the forefront of this study is an analysis of U.S. policy evolution pertaining CIs and cyber security, a detailed look at the 16 U.S. CI sectors, an examination of the reliance of CIs on computer technology, and an exploration of the vulnerability and potential consequences of cyber attacks on U.S. CIs.

2. Why Stuxnet was Chosen

The Stuxnet attack provides an outline for how to conduct a specifically targeted cyber-warfare attack on the computer systems of a state run CI target.[15] The Stuxnet worm was chosen because it is the first publicly known use of a cyber weapon to destroy the CI of another country. Stuxnet effectively accomplished, with computer malware deployment, what traditionally was only possible through bombing or traditional sabotage.[16] Stuxnet presents a unique

---

[13] David Kushner, "The Real Story of Stuxnet," *IEEE Spectrum*, February 1, 2013, http://spectrum.ieee.org/telecom/security/the-real-story-of-stuxnet.

[14] Steve Kroft, "Stuxnet: Computer Worm Opens New Era of Warfare," CBS News, June 1, 2012, http://www.cbsnews.com/news/stuxnet-computer-worm-opens-new-era-of-warfare-04-06-2012/.

[15] Karnouskos, "*Stuxnet Worm Impact on Industrial Cyber-Physical System Security*."

[16] David Sanger, "Obama Order Sped Up Wave of Cyberattacks Against Iran," *The New York Times*, May 31, 2012, http://www.nytimes.com/2012/06/01/world/middleeast/obama-ordered-wave-of-cyberattacks-against-iran.html?pagewanted=all&_r=0.

opportunity for study because it is relevant to CI cyber vulnerability in the U.S. today and has a great deal of unclassified information available on the topic.

3. Limitations

The purpose of this paper is not to distill the speculative writing as to whom or which government was actually responsible for the deployment of Stuxnet. This study focuses on the functional deployment of Stuxnet, the vulnerabilities it exploited, its effects on a high security CI, and policy recommendations for U.S. CIs.

D. LITERATURE REVIEW

1. Introduction

The literature reviewed for this thesis, centered around the Stuxnet attack on Iran's Natanz uranium enrichment facility, is very diverse. It includes national policies from several countries, CI specific information, technical information concerning ICS, documents detailing the Stuxnet attack itself and an array of documents and literature contemplating the ramifications of the Stuxnet attack. A wide net must be cast to capture the background information needed to understand fully what this attack means to U.S. CIs and national policy. A wide variety of literary sources have been incorporated into this project to include books, technical publications, scholarly journal articles, published scholarly research papers, media reports, studies sponsored by organizations and Internet publications. The literature was assessed and then categorized by content type, although many sources contain information that fits neatly into multiple categories.

This research topic is important for three reasons. First, the Stuxnet attack allows for a rare case study into a verifiable cyber attack on a government controlled CI. Literature available is on this attack in the non-classified realm, which might not be the case for most such attacks. Second, Stuxnet specifically targeted the ICS of the Natanz facility. Many U.S. CI sectors rely heavily on ICS.

Finally, parallels can be drawn between the Stuxnet attack in Iran and U.S. CI vulnerability. Examining these parallels will lead to policy recommendations for strengthening the U.S. posture as it pertains to the cyber protection of national CIs.

Two important definitions are key to understanding the concepts related to this subject matter.

- *Critical Infrastructure* (CI)—The Department of Homeland Security (DHS) defines CIs as, "The assets, systems, and networks, whether physical or virtual, so vital to the United States that their incapacitation or destruction would have a debilitating effect on security, national economic security, national public health or safety, or any combination thereof."[17]

- *Industrial Control System* (ICS)—"Combinations of control components that act together to achieve an industrial objective."[18]

Overall, the literature on CIs and ICS is a mature array of documents with useful sources dating as far back as 1996. However, the literature on the Stuxnet attack itself is a different story. This attack was uncovered within the past five years; thus, the literature is relatively recent, with new material still being actively produced. Multiple relevant sources from 2014 and 2015 were found and utilized during research for this thesis, which sets the literature lifespan for the materials reviewed for this thesis at the past 20 years.

The pertinent literature is organized into the following five categories:

- Policy documents
- U.S. CIs
- Industrial control systems
- Stuxnet attack
- Future ramifications of Stuxnet

[17] "What Is Critical Infrastructure?," last modified October 24, 2013, http://www.dhs.gov/what-critical-infrastructure.

[18] Stouffer et al., *Guide to Industrial Control Systems Security*, 17.

2. Policy Documents

The objective of this thesis is to identify the pivotal areas of U.S. CI cyber protection policy that could be enhanced to provide the most effective solutions to the current vulnerabilities highlighted by the Stuxnet attack on Iran, and provide corresponding recommendations to improve U.S. policy. A review of U.S. national policy documents is a prerequisite for being able to recommend policy improvements. Large collections of pertinent documents were reviewed to include legislation, commission reports, presidential decision directives, executive orders and official federal plans.

Executive Order (EO) 13010, signed by President Clinton on July 5, 1996, may be viewed as a starting point for U.S. CI protection. CI was defined and the initial CI sectors were identified. On May 22, 1998, President Clinton signed Presidential Decision Directive (PDD) 63, which focused on the subject of "CI protection."[19] This directive identified CI as a growing vulnerability and assigned each CI sector primary federal agency responsibility.

President George W. Bush published two key executive orders, during the post-September 11th era, relevant to CI protection. EO 13228, signed by President Bush October 8, 2001, established the Office of Homeland Security and the Homeland Security Council.[20] Eight days later, on October 18, 2001, he signed EO 13231. This document, entitled "Critical Infrastructure Protection in the Information Age," profoundly shifts the federal focus toward cyber threats.

In October 2012, President Obama authorized Presidential Policy Directive 20, which defined U.S. cyber operations policy.[21] The directive was issued as a classified document with a public fact sheet, but was later leaked and interpreted in a newspaper article by national security reporter Ellen Nakashima,

---

[19] White House Office of the Press Secretary, *Critical Infrastructure Protection*, Presidential Decision Directive 63, Washington, DC: The White House Office of the Press Secretary, 1998, 1.

[20] Exec. Order No. 13228, 66 FR 51812 (2001-03), 1.

[21] Catherine A. Theohary and Anne I. Harrington, *Cyber Operations in DOD Policy and Plans: Issues for Congress* (CRS Report No. R43848) (Washington, DC: Congressional Research Service, 2015), 18, http://fas.org/sgp/crs/natsec/R43848.pdf.

of the *Washington Post*.[22] President Obama issued EO 13636, in February 2013, which was entitled "Improving Critical Infrastructure Cybersecurity."[23] This order identifies repeated cyber intrusions into critical infrastructure as a growing threat that must be confronted.

Presidential Policy Directive 21 (PPD 21), "Critical Infrastructure Security and Resilience," accompanied the release of EO 13636 in February 2013. PPD 21, "Establishes national policy on critical infrastructure security and resilience."[24] PPD 21 also required an update to the National Infrastructure Protection Plan (NIPP). The resulting work product was the NIPP 2013.

EO 13636 called for, "the development of a voluntary risk based Cybersecurity Framework."[25] The objective of the framework was to collaboratively develop a, "set of industry standards and best practices to help organizations manage cybersecurity risks."[26] The NIST published the resulting framework in February 2014.[27]

Comparisons must be drawn with the CI cyber security policy strategies of other nations to gauge the effectiveness of U.S. policies. The Australian government published complimentary documents in back to back years to focus on private and government sector stakeholders within this mission space. In 2009, Attorney General Robert McClelland published the Australian national "cyber security strategy" to synergize efforts on national objectives to protect the

---

[22] Ellen Nakashima, "Obama Signs Secret Directive to Help Thwart Cyberattacks," *Washington Post*, November 14, 2012, https://www.washingtonpost.com/world/national-security/obama-signs-secret-cybersecurity-directive-allowing-more-aggressive-military-role/2012/11/14/7bf51512-2cde-11e2-9ac2-1c61452669c3_story.html.

[23] Exec. Order No. 13636, 78 FR 11739 (2013), 1.

[24] The White House Office of the Press Secretary, *Critical Infrastructure Security and Resilience,* Presidential Decision Directive 21, Washington, DC: The White House Office of the Press Secretary, 2013, 2.

[25] National Institute of Standards and Technology, *Framework for Improving Critical Infrastructure Cyber Security* (Gaithersburg, MD: National Institute of Standards and Technology, 2014), 1.

[26] Ibid.

[27] Ibid.

Australian government, and business and civilian sectors from cyber threats. The document also specifically addresses ICS security[28] and CI cyber protection.[29] In 2010, he published the complimentary Australian national "critical infrastructure resilience strategy," detailing an all hazards approach to national CI resiliency with an emphasis on cyber threats. These two policy documents outline overarching frameworks Australians can use to understand the objectives, strategic priorities, and components of their national strategy.

The United Kingdom (U.K.) published a comprehensive national policy document, outlining a five-year strategy, on November 25, 2011. The policy is entitled, "The UK Cyber Security Strategy: Protecting and Promoting the UK in a Digital World," and notes that the U.K.'s national security strategy includes cybersecurity as one of its top tier national priorities. The strategy requires annual progress report updates at the end of each year that measure progress toward published program objectives. The United Kingdom also implemented a voluntary "cyber essentials" program in 2014 to reward cyber security best practices among private sector businesses. This government backed and industry supported program incentivizes widespread adoption of cyber security best practices that protect organizations against cyber attacks and gives them the ability to differentiate themselves in the marketplace for customers, investors, and business partners.

3. U.S. Critical Infrastructures

This thesis dissects the Stuxnet attack to derive policy recommendations to improve the cyber resilience of U.S. CIs. Therefore, a base of knowledge must be constructed concerning U.S. CIs. A review of the pertinent literature turned up several different types of sources, which are helpful in this regard. Useful materials ranging from PPD 21, to Congressional Research Service (CRS)

[28] Commonwealth of Australia, *Cyber Security Strategy* (Commonwealth of Australia: Attorney General's Department, 2009), 13, https://www.ag.gov.au/RightsAndProtections/CyberSecurity/Documents/AG%20Cyber%20Security%20Strategy%20-%20for%20website.pdf.

[29] Ibid., 20.

reports, to the websites sponsored by the DHS all cover different aspects of U.S. CIs.

The key foundational document found on CIs in the United States is PPD 21. This document was published on February 12, 2013, and is intended to establish national policy on CI security and resilience. The directive maps out the 16 recognized U.S. CI sectors and establishes policy guidance for their protection. Although the document spends considerable space laying out federal obligations, it also emphasizes that the responsibility for protecting these assets is shared with state and local government agencies along with the owners and operators of privately owned facilities. This shared responsibility is a cornerstone concept for the policy recommendations that conclude this thesis.

The CRS has published a number of reports on different aspects of this topic, which are outstanding sources of information. In January 2004, the CRS published a paper entitled *Critical Infrastructure: Control Systems and the Terrorist Threat*. Although this report might seem dated, it has strong historical context that documented CI vulnerability to cyber attacks over a decade ago. The report also ties this topic in to the original USA Patriot Act and sets the stage for the assertion that this vulnerability is not completely new.

Another very topical CRS report was published in December of 2010 entitled, *The Stuxnet Computer Worm: Harbinger of an Emerging Warfare Capability*. This report is helpful in not only documenting concerns about U.S. CIs, but also connecting them to potential vulnerabilities a Stuxnet style attack could potentially exploit. As a bonus for other portions of the thesis, this report also contains specific information on the Stuxnet attack and its effects on Iran.

The DHS has a website dedicated to publishing information for the Industrial Control Systems Cyber Emergency Response Team. Their function is to provide a coordinated defense of national ICS against emerging cyber threats and to share information with public and private stakeholders. This website is full of topical advisories, alerts, newsletters, and reports that relate directly to this

thesis topic. In addition, the DHS maintains a web page portfolio analyzing each of the 16 CI sectors. These pages include detailed sector specific information that provides critical context to the differences in vulnerability between the various sectors.

4. Industrial Control Systems

ICS are a critical computerized component of many U.S. CIs. To understand the vulnerabilities present within these systems, it is necessary to have a foundational understanding of these systems and how they function within the CI environment. Much of the literature within this category is very technical and tends to be associated with professional or trade publications.

Tarun Agarwal wrote several articles for "EDGEFX.US," including an article entitled "A Glance on Industrial Control Systems with Control Strategies." This article does a nice job breaking down a complex topic into easy to digest sections. One particularly useful section entitled "Types of Industrial Control Systems," breaks these systems down into three categories and explains what these different systems control as it pertains to industrial processes.

German researcher Stamatas Karnouskos published a paper entitled, "Stuxnet Worm Impact on Industrial Cyber-Physical System Security." This paper covers ICS and the vulnerabilities inherent within their environments. He notes a false sense of security that he believes is present with managers of these isolated network systems. Karnouskos also points to aging and poorly defended industrial infrastructures as an easy target for malware attacks.

Gheorghe Boaru and George-Ionut Badita, of the Romanian National Defense University, authored a paper directly applicable to this thesis entitled, "Critical Infrastructure Protection Challenges and Efforts to Secure Control Systems." This material directly applies to multiple sections of this thesis to include the role of ICS in electricity generation and distribution, the cyber vulnerabilities of current ICS, automated decision making by ICS, and the perceived logic behind private sector reluctance to upgrade or update their ICS.

A CRS report from Dana Shea entitled, *Critical Infrastructure: Control Systems and the Terrorist Threat*, provides foundational information on how ICS function and fit into CIs. The information is presented in a manner easily understood by readers who may not come from a technical or engineering background. Morgan Henrie wrote an article entitled "Cyber Security Risk Management in the SCADA Critical Infrastructure Environment," for the *Engineering Management Journal*. This article provides detailed information on how SCADA systems remotely monitor multiple field sites and take autonomous action during industrial processes.

The NIST published a definitive report in May 2014 entitled, *Guide to Industrial Control Systems Security* (NIST Special Publication 800–802). It is a comprehensive report, directly related to this thesis topic, which is a key building block for this thesis. The report provides an operational overview of the functions and types of ICS, a section on ICS risk management, a section on ICS security architecture and other important information, such as an acronym appendix for this technical subject matter.

5. The Stuxnet Attack

The Stuxnet attack was not discovered until 2010; therefore, the literature on the attack itself is still being written. The author found some of the best information on the Stuxnet attack in technology industry publications and news sources. Some of those news stories in turn began to emerge as books, such as David Sanger's, *Confront and Conceal: Obama's Secret Wars and Surprising Use of American Power*. Although this book contains good information about the Stuxnet attack, a researcher must realize that this book has a political agenda behind it and scrutinize it for editorial content as opposed to factual content. Factual information can also be extracted from the newspaper articles Sanger authored prior to the release of this book.

The Institute of Electrical and Electronics Engineers (IEEE) shares information in its online publication entitled *Spectrum*. In February 2013, *IEEE*

Spectrum published an article by David Kushner entitled, “The Real Story of Stuxnet.” This report is rich with a lot of factual information from an unbiased industry perspective. Kushner details the discovery, size, and scope of Stuxnet, along with the three phases with which it was deployed. The article also explains how the worm could be spread to systems not part of a network and identifies Chevron as the first U.S. corporation to admit that Stuxnet had infected it’s systems. The author also provides a useful “milestones in malware” timeline of significant malware events since 1971. Kushner also takes a look ahead at new malware threats and U.S. ICS vulnerability.

The *Washington Post* published a series of investigative pieces on Stuxnet from 2010–2012. Several of these articles are directly applicable to this research. Ellen Nakashima’s article, “Stuxnet Malware is a Blueprint for Computer Attacks on U.S.” (October 2010), specifically covers how a similar attack could sabotage computer equipment critical to U.S. power plants, power grids, and other infrastructures. The article contains interviews and quotes about Stuxnet from both industry and government experts. Joby Warrick’s investigative piece, “Iran’s Natanz Nuclear Facility Recovered Quickly from Stuxnet Cyberattack” (February 2011), explains how United Nations (UN) inspectors had a front row seat to watch Stuxnet’s damage to Natanz through cameras that were in place to monitor the facility under a weapons monitoring program. Nakashima and Warrick combined forces in 2012 for follow up articles that expand on their earlier works.

The author found additional research materials in investigative articles written and published by *Reuters*, *Business Insider* and *The New York Times*. David Sanger first started publishing his investigative pieces in *The New York Times* prior to publishing his book. His article, “Obama Sped Up Wave of Cyberattacks against Iran,” contains good information on the phases of the attack and the effects on Natanz. This article also lays out his theory for how Stuxnet spread from Natanz to the Internet. The articles from *Reuters* and *Business*

Insider are less comprehensive than the others but contain some pertinent technical details not found in other sources.

Ralph Langer is a German ICS security expert who has achieved recognition for his analysis of Stuxnet. He published part of his analysis in a document entitled, “To Kill a Centrifuge,” which although it is very technical in spots, provides a detailed breakdown of the Stuxnet attack that is directly pertinent to this thesis. Langer details the three layers of ICS that must be interacted with to accomplish physical damage with a cyber attack. He also elaborates on the resources necessary to develop and implement a cyber attack of Stuxnet’s magnitude and covers the specific vulnerabilities the attack sought to exploit.

Other technical documents, such as Symantec’s “W32.Stuxnet Dossier,” provide outstanding functionality details, such as how Stuxnet propagated itself, and outlines specific points of failure within Natanz that allowed Stuxnet to flourish in Iran. Jim E. Crouch and Larry K. McKee Jr., of the National Security Cyberspace Institute, published a report entitled, “Cybersecurity: What Have We Learned?” This report covers how specific policy approaches can be utilized to prevent attacks like Stuxnet. Doug Niblick’s “Protecting Critical Infrastructure against the Next Stuxnet” also covers policy and technical issues key to preventing CI cyber attacks.

6. Future Ramifications of Stuxnet

The last portion of this initial literature review deals with what Stuxnet means, moving forward, for U.S. CIs and the policies that affect them. Stuxnet casts a long shadow on this complex and interdependent network of vital assets. Many of the literary sources already detailed have sections that directly apply to this portion of this thesis as well.

In June 2012, CBS News aired a feature 60 Minutes segment entitled, “Stuxnet: Computer Worm Opens New Era of Warfare.” This comprehensive investigative report covered the basics, such as the how Stuxnet was discovered,

and how it worked. However, it also took a predictive look at what Stuxnet foretells for the future of the United States through the eyes of key decision makers at that time, such as Federal Bureau of Investigation (FBI) Director Robert Mueller, Defense Secretary Leon Panetta, House Intelligence Committee Chairman Mike Rogers, and Retired General Mike Hayden.

A number of news articles were located with information pertinent to the future ramifications of Stuxnet. Ellen Nakashima's work with the *Washington Post* surfaces again with her piece entitled, "Hacks of OPM Databases Compromised 22.1 Million People, Federal Authorities Say." It is another directly applicable article that can be used to show that the United States still has current unaddressed cyber vulnerabilities being actively exploited by adversaries. *The Wall Street Journal* published a pertinent article entitled, "Cyberwar Ignites New Arms Race," which provides an overview of nations currently fielding either military- or intelligence-based cyber units to conduct operations in cyber space. It also details the current U.S. military posture pertaining to cyber units and reveals staffing plans for their expansion in the near future. *News 24* published an article in May 2012 entitled, "Cyber Terror Targets Utilities." This article covers everything from energy infrastructure vulnerability to theories about cyber attacks becoming a staple in modern warfare. More specifically, it contains opinions from industry experts who believe that energy and communications networks would be considered desirable targets to begin any modern day military attack.

Catherine Theohary and Anne Harrington of the CRS authored a report entitled, *Cyber Operations in DOD Policy and Plans: Issues for Congress*, which focuses on the policy dilemmas U.S. decision makers will have to wrestle with in the near future. The U.S. Government Accountability Office (GAO) published a report entitled, *Critical Infrastructure Protection- Progress Coordinating Government and Private Sector Efforts Varies by Sectors' Characteristics*. This insightful article provides statistical information pertinent to CI cyber vulnerability, what has been done, and where more progress is required. Amitai Etzioni, of the George Washington University, published an article entitled, "The Private Sector:

A Reluctant Partner in Cybersecurity." This article clearly articulates the reasoning why some private sector CI stakeholders are slow to upgrade cyber security technology in their facilities.

Research revealed two other topics with consequential future implications related to cyber security for CIs. The first topic concerns the ethical issues that arise from taking action in cyberspace. Dorothy Denning of the Naval Postgraduate School wrote a paper entitled, "Framework and Principles for Active Cyber Defense." This paper focuses on covering the differences between active and passive cyber countermeasures and the ethical dilemmas than arise from taking action in cyberspace. An edited book with chapters from multiple authors entitled, "Warfare in a New Domain: Ethics of Military Cyber-Operations," takes a deeper dive into these ethical issues from the perspectives of multiple authors. Although many of these chapters are militarily based, many parallels can be drawn with government and private sector CI cyber protection.

The second topic of consequential implications for the future of cyber defense concerns the educational sector. The United States is struggling to educate and train sufficient numbers of cyber security professionals. *Defense Horizons* published an article entitled, "Preparing the Pipeline: The U.S. Cyber Workforce for the Future." This article lays out the cornerstone educational fields where focus is needed to build a competent cyber security workforce and details difficulties currently found within the industry to meet staffing demands. Christophe Veltsos authored an article entitled, "Addressing the Information Security Skills Gap in Partnership with Academia," for *Security Intelligence* in October 2015. Veltsos describes a gap in the U.S. cyber security workforce that results from U.S. educational institutions failing to train and educate cyber security professionals fast enough to meet the demand. He describes a professional environment in which private and public sectors employers are forced to raid cyber security talent from competitors or government agencies because not enough qualified professionals are available to meet national needs.

The Unisys Corporation partnered with the Ponemon Institute to conduct a survey of 599 executives in key industries, such as utilities, oil and gas, energy, and manufacturing. The survey questions probed the executives' views of ICS vulnerability within their companies. This survey contains remarkable responses that highlight the wide scope of CI cyber vulnerability. The survey responses paint the portrait of a recognized problem not being appropriately prioritized for solutions. The CSIS Strategic Technologies Program published a noteworthy "Cyber Incident Timeline," which chronicles significant cyber attacks, and aides in scoping the breadth of current CI vulnerabilities.

The author's literature research of U.S. policy, U.S. CIs, ICS, Stuxnet's deployment, and future policy ramifications resulting from the Stuxnet attack, was a continual and evolving process. During this thesis project, a point was never reached when the research was considered to be "complete." It is still an emergent topic and new sources and articles were found daily during the research process right up until the end of the project. This topic will continue to be fertile ground for further research into the foreseeable future.

E. CONTRIBUTION TO THE HOMELAND SECURITY ENTERPRISE

The technical vulnerabilities of CI computer systems have been a topic of increasing concern for government, technology, and computer security experts. The objective of this thesis is to identify the pivotal areas of U.S. CI cyber protection policy that could be enhanced to provide the most effective overarching solutions to the current vulnerabilities highlighted by the Stuxnet attack on Iran, and provide subsequent recommendations for U.S. policy advancements. This thesis provides a unique opportunity to study the use of a cyber weapon to target CI, in an unclassified environment, for the benefit of homeland security professionals from all disciplines.

THIS PAGE INTENTIONALLY LEFT BLANK

II. U.S. POLICY

Government agencies have been concerned about CI security in the United States for decades. Those concerns range from physical threats, such as the September 11, 2001, airline hijackings that led to the death of thousands of Americans, and the destruction of the World Trade Center, to an increasing focus on cyber threats. Certain socioeconomic activities form the foundation of day-to-day life and shape the overall security posture of this nation. Some of these activities include the transportation of goods and people, functioning communications networks, banking and finance, and the supply of basic necessities, such as electricity and water.[30] Interruptions to the delivery of these services can have a disruptive effect on this nation's well-being and psyche. The infrastructures required to deliver these services have grown to be increasingly complex, interconnected and reliant on networked computer systems. In a cascading effect, the disruption on one system may lead to the disruption of others.[31]

A. CYBER ATTACKS AND CRITICAL INFRASTRUCTURE

The 1990s, and the first decade of this century, saw a primary focus on three negative consequences of fast-growing web and networked computer technology. Those areas included cyber crime, espionage, and the theft of intellectual property.[32] See Figure 1. However, ominous clouds were on the horizon signaling potential new threats. The National Security Agency (NSA) conducted an internal exercise that began in 1997 dubbed "Eligible Receiver." The exercise exposed, for the first time, just how ill prepared the United States

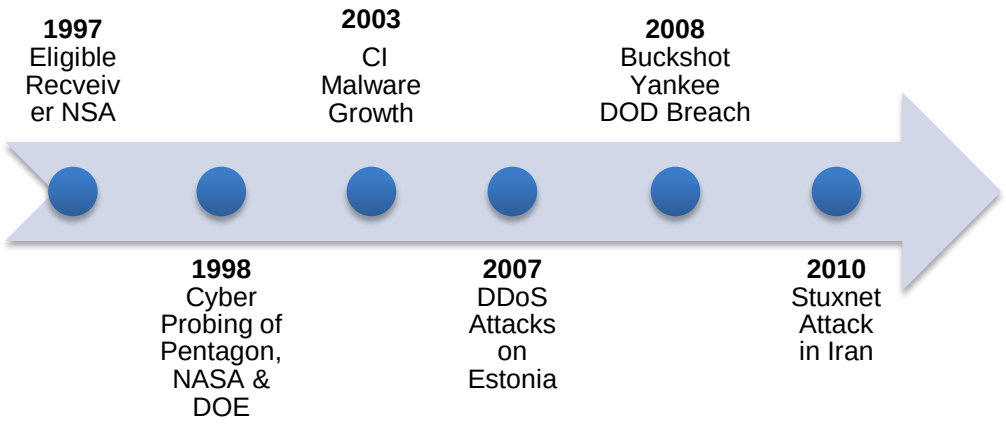
[30] John D. Moteff, *Critical Infrastructures: Background, Policy, and Implementation* (CRS Report No. RL30153) (Washington, DC: Congressional Research Service, 2015), 2, http://fas.org/sgp/crs/homesec/RL30153.pdf.

[31] Ibid., 1.

[32] Misha Glenny and Camino Kavanagh, "800 Titles but no Policy—Thoughts on Cyber Warfare," *American Foreign Policy Interests* 34, no. 6 (2012): 287, http://search.proquest.com.libproxy.nps.edu/docview/1264925856?accountid=12702.

was to protect computer networked CIs from cyber attacks.[33] NSA hackers used publicly available material to infiltrate the Department of Defense's (DOD's) Pacific Command Center successfully, this nation's electric grids and 9-1-1 emergency communications systems in nine major cities.[34] In 1998, the United States uncovered a cyber-probing program that had been accessing the computer networks of the Pentagon, the National Aeronautics and Space Administration, the Department of Energy (DOE) and select university research labs. The two-year long campaign was traced back to a mainframe computer in the former Soviet Union.[35] A series of malware worms, designed for espionage and surveillance, or CI targets, were discovered throughout 2003.[36]

Figure 1. Timeline of Significant Early Cyber Events



Ethnic strife within Estonia, between ethnic Estonians and Russia nationals, led to social unrest and crippling distributed denial of service attack

[33] Glenny and Kavanagh, "800 Titles but no Policy—Thoughts on Cyber Warfare," 287.

[34] Ibid., 288.

[35] Bob Drogin, "Russians Seem to be Hacking into Pentagon," *Los Angeles Times*, October 7, 1999, http://www.sfgate.com/news/article/Russians-Seem-To-Be-Hacking-Into-Pentagon-2903309.php.

[36] Glenny and Kavanagh, "800 Titles but no Policy—Thoughts on Cyber Warfare," 287.

(DDoS), which affected the nation's CI and government access to the Internet.[37] The U.S. and European allies debated whether the Estonian cyber attack was an act of cyber warfare or digital violence that required new countermeasures. The DDoS strike effectively halted public services, commerce, and government operations.[38] Although it was widely believed that Russian hackers were responsible for the attacks, direct attribution to the Kremlin was not achieved.[39] That incident was followed up by a 2008 malware compromise of DOD computer networks by a "foreign intelligence agency." The malware was implanted via an infected universal serial Bus (USB) memory stick and spread through the military's unclassified network and classified networks prompting a response launched under the code name "Buckshot Yankee." This wakeup call was the most serious historical compromise of U.S. military networks ever, at that time, and could have led to the delivery of battle plans into the hands of a foreign adversary.[40]

Securing cyberspace, and the computer networked CIs which interact within it, has become a national policy priority for many governments, including the United States. For now, state actors and inter-state relationships rule within the cyber realm. However, the potential for terrorist groups to develop the capability or relationships necessary to target a nation's government and private CIs remains a serious threat. Government and industry experts agree that once terrorists acquire the necessary skills and sophistication, they will use it.[41]

---

[37] Stephen Herzog, "Revisiting the Estonian Cyber Attacks: Digital Threats and Multinational Responses," *Journal of Strategic Security* 4, no. 2 (Summer 2011): 50–51, http://scholarcommons.usf.edu/cgi/viewcontent.cgi?article=1105&context=jss.

[38] Ibid., 54.

[39] Ibid., 53.

[40] William J. Lynn III. "Defending a New Domain," *Foreign Affairs*, accessed November 29, 2015, https://www.foreignaffairs.com/articles/united-states/2010-09-01/defending-new-domain.

[41] Natalia Tereshchenko, "U.S. Foreign Policy Challenges of Non-State Actors' Cyber Terrorism against Critical Infrastructure," *International Journal of Cyber Warfare and Terrorism* 2, no. 4 (October 2012): 29, http://search.proquest.com/docview/1465900385?accountid=12702.

B. EVOLUTION OF U.S. POLICY ON CYBER CI PROTECTION

Defining U.S. policy as it pertains to CI cyber protection is made difficult due to the overlapping nature of the various documents, which make up the policy. The complex policy must be distilled from differing documents, such as legislation, commission reports, presidential decision directives, EOs and official federal plans. Changes in Presidential administrations bring a cycle of restructuring, realigning, renaming, and refocusing of efforts and objectives.

The modern era of CI protection and cyber defense began under President William J. Clinton. EO 13010, signed by President Clinton on July 5, 1996, may be viewed as a starting point for U.S. CI protection. CI was defined and the initial CI sectors were identified. The order established the "President's Commission on Critical Infrastructure Protection" and set up the "Principals Committee" to review their recommendations prior to submission to the President.[42] The Commission recommended greater cooperation and communication between the government and the private sector, and generally viewed information dissemination on intrusion techniques, threat analysis, and computer hacker defense, as its primary role.[43] This theme of encouraging greater collaboration between the private and government sectors is a common anchor of all the policy documents reviewed during this research.

On May 22, 1998, President Clinton signed PDD-63, which focused on the subject of "CI protection."[44] This directive identified CI as a growing vulnerability, assigned each CI sector primary federal agency responsibility, and required the creation of a National Infrastructure Assurance Plan that would integrate protection plans from the CI sectors. A 180-day timeframe was set for the completion of the plan, related vulnerability analyses, and sector specific

[42] Exec. Order No. 13010, 61 FR 37347 (1996–99), 1.

[43] Moteff, *Critical Infrastructures: Background, Policy, and Implementation*, 3.

[44] White House Office of the Press Secretary, *Critical Infrastructure Protection*, Presidential Decision Directive 63, 1.

remedial plans.[45] PDD-63 also displayed heightened cyber security awareness and compelled enhancements to U.S. proficiency in the diagnosis and timely countering of cyber attacks.[46] The criticality of public and private partnerships again was identified as a key strategic component to reducing critical infrastructure vulnerability.[47]

President George W. Bush published two key EOs during the post September-11 era that were relevant to CI protection. EO 13228, signed by President Bush on October 8, 2001, established the Office of Homeland Security and the Homeland Security Council.[48] The Office of Homeland Security was required to develop and implement a comprehensive national strategy to secure the nation's CIs from terrorist threats.[49] The Homeland Security Council was set up to advise the President on all homeland security matters.[50]

Eight days later, on October 18, 2001, President Bush signed EO 13231. This document, entitled "Critical Infrastructure Protection in the Information Age," profoundly shifts the federal focus toward cyber threats. It recognizes that technology has transformed the way society functions and was published specifically to ensure protection of information systems for CI.[51] The order also establishes the "President's Critical Infrastructure Protection Board" to propose new guidelines and organize initiatives designed to safeguard the computer networks of U.S. CIs. The chairman of that board was designated to act as a Special Advisor to the President for Cyberspace Security.[52]

---

[45] White House Office of the Press Secretary, *Critical Infrastructure Protection*, Presidential Decision Directive 63, 8.

[46] Moteff, *Critical Infrastructures: Background, Policy, and Implementation*, 6.

[47] The White House Office of the Press Secretary, *Critical Infrastructure Protection* Presidential Decision Directive 63, 3.

[48] Exec. Order No. 13228, 66 FR 51812 (2001–03), 1.

[49] Ibid.

[50] Ibid.

[51] Exec. Order No. 132231, 66 FR 53063 (2001), 1.

[52] Ibid., 4.

In January 2008, President Bush signed National Security Presidential Directive 54/Homeland Security Presidential Directive 23 requiring a cyberspace policy review. President Obama subsequently took office in January 2009, identified cyber security as a national security threat, and directed that all computer infrastructures within the purview of the federal government be comprehensively reviewed.[53] He later authorized the guidance published following the Bush initiated cyber space policy review, in May 2009. It included the establishment of an "Executive Branch Cybersecurity Coordinator," who would have direct access to the president.[54]

Although the initial directive was published as classified, the resulting "Comprehensive National Cybersecurity Initiative" (CNCI) document was not. President Obama viewed the CNCI as playing a key role in supporting his cybersecurity objectives.[55] The report sought unity of effort in national cybersecurity efforts. The CNCI sets three major goals to help secure the United States in cyberspace.

The first goal of the CNCI is, "to establish a front line of defense against today's immediate threats by creating or enhancing shared situational awareness of network vulnerabilities, threats, and events within the Federal Government—and ultimately with state, local, and tribal governments and private sector partners."[56] This unified front line of defense would have the shared, "ability to act quickly to reduce our current vulnerabilities and prevent intrusions."[57]

---

[53] Executive Office of the President of the United States*, The Comprehensive National Cybersecurity Initiative* (Washington, DC: Executive Office of the President of the United States, 2009), 1.

[54] Ibid.

[55] Ibid.

[56] Ibid.

[57] Ibid.

The second goal of the CNCI is, “to defend against the full spectrum of threats by enhancing U.S. counterintelligence capabilities and increasing the security of the supply chain for key information technologies.”[58]

The third goal of the CNCI is, “to strengthen the future cybersecurity environment by expanding cyber education; coordinating and redirecting research and development efforts across the Federal Government; and working to define and develop strategies to deter hostile or malicious activity in cyberspace.”[59]

In October 2012, President Obama authorized PPD 20, which defined U.S. cyber operations policy.[60] The directive was issued as a classified document with a public fact sheet, but was later leaked and revealed in a newspaper article by national security reporter Ellen Nakashima, of the *Washington Post*.[61] Nakashima interviewed un-named senior administration officials, who were not authorized to speak on the record, about the document and its contents. According to Nakashima, PPD 20 establishes a framework of standards to guide the actions taken by federal agencies manning the battle lines of emerging cyber threats.[62] The author characterizes the document by writing it, “attempts to settle years of debate among government agencies about who is authorized to take what sorts of actions in cyberspace and with what level of permission.”[63] She continues by writing, “For the first time, the directive explicitly makes a distinction between network defense and cyber-operations to guide

---

[58] Executive Office of the President of the United States*, The Comprehensive National Cybersecurity Initiative*, 1.

[59] Ibid.

[60] Theohary and Harrington*. Cyber Operations in DOD Policy and Plans: Issues for Congress*, 18.

[61] Nakashima, “Obama Signs Secret Directive to Help Thwart Cyberattacks.”

[62] Ibid.

[63] Ibid.

officials charged with making often-rapid decisions when confronted with threats."[64]

In part, the public White House fact sheet for PPD 20 notes that it "establishes principles and processes for the use of cyber operations to ensure our cyber tools are integrated with the full array of national security tools we have at our disposal."[65] The fact sheet adds that PPD 20, "provides a whole-of-government approach consistent with the values our nation that we promote domestically and internationally."[66] The PPD 20 fact sheet also establishes that it will be U.S. policy, "that we shall undertake the least action necessary to mitigate threats and that we will prioritize network defense and law enforcement as the preferred courses of action."[67]

President Obama issued EO 13636, in February 2013, which was entitled "Improving Critical Infrastructure Cybersecurity."[68] This order identifies repeated cyber intrusions into CI as a growing threat that must be confronted. EO 13636 states, "it is the policy of the United States to enhance the security and resilience of the nation's critical infrastructure and to maintain a cyber environment that encourages efficiency, innovation, and economic prosperity while promoting safety, security, business confidentiality, privacy, and civil liberties."[69]

This document focuses on the challenges presented by privately owned and operated CIs, and the need to share information with them. EO 13636 stresses the importance of, "partnerships with the owners and operators of critical infrastructures to improve cybersecurity information sharing and

---

[64] Nakashima, "Obama Signs Secret Directive to Help Thwart Cyberattacks."

[65] The White House Office of the Press Secretary, *Cyber Operations,* Presidential Decision Directive 20 (Fact Sheet Only), Washington, DC: The White House Office of the Press Secretary, 2013, 1.

[66] Ibid.

[67] Ibid.

[68] Exec. Order No. 13636, 78 FR 11739 (2013), 1.

[69] Ibid., 2.

collaboratively develop and implement risk based standards."[70] It further identifies as a policy objective of the U.S. government to, "increase the volume, timeliness, and quality of cyber threat information shared with U.S. private sector entities," so they may "better protect and defend themselves against cyber threats."[71]

The policy focus on productive information sharing is further supported in this document through direction to ensure the "dissemination of classified reports to critical infrastructure entities authorized to receive them," and expediting "the processing of security clearances for appropriate personnel employed by critical infrastructure operators."[72] EO 13636 also calls for the expanded "use of programs that bring private sector subject matter experts into federal service on a temporary basis" to increase productive collaboration between the government and private sectors.[73]

EO 13636 also called upon the Secretary of Commerce to task the director of NIST with developing a "cybersecurity framework," to address cyber vulnerability within national CI. The framework was to include input from private sector stakeholders to encourage participatory compliance with collaboratively established cyber security best practices.[74] The framework was directed to specifically provide for a, "flexible, repeatable, performance-based, and cost-effective approach, including information security measures and controls, to help owners and operators of critical infrastructure identify, assess and manage cyber risk."[75] The order also directs the Secretary of Homeland Security to implement a "voluntary critical infrastructure cybersecurity program" to incentivize the

[70] Exec. Order No. 13636, 78 FR 11739 (2013), 2.

[71] Ibid.

[72] Ibid., 3.

[73] Ibid.

[74] Ibid., 5.

[75] Ibid.

utilization of the "cybersecurity framework" among private sector CI stakeholders.[76]

PPD 21, "Critical Infrastructure Security and Resilience," accompanied the release of EO 13636 in February 2013. PPD 21, "Establishes national policy on critical infrastructure security and resilience."[77] It also notes that this responsibility is, "shared among federal, state, local, tribal, territorial entities, and private owners of critical infrastructure." The policy statement reads as follows:

> It is the policy of the United States to strengthen the security and resilience of its critical infrastructure against both physical and cyber threats. The Federal Government shall work with critical infrastructure owners and operators and SLTT entities to take proactive steps to manage risk and strengthen the security and resilience of the Nation's critical infrastructure, considering all hazards that could have a debilitating impact on national security, economic stability, public health and safety, or any combination thereof. These efforts shall seek to reduce vulnerabilities, minimize consequences, identify and disrupt threats, and hasten response and recovery efforts related to critical infrastructure.[78]

PPD 21 promotes "three strategic imperatives" that govern U.S. strategy toward bolstering CI security and resilience.[79] The first imperative forwarded within PPD 21 is to, "refine and clarify functional relationships across the Federal Government to advance national unity of effort to strengthen critical infrastructure security and resilience." The second imperative from PPD 21 is to, "enable effective information exchange by identifying baseline data and systems requirements for the Federal Government." The final imperative of PPD 21 is to, "implement an integration and analysis function to guide planning and operational decisions regarding critical infrastructure."

---

[76] Exec. Order No. 13636, 78 FR 11739 (2013), 6.

[77] The White House Office of the Press Secretary, *Critical Infrastructure Security and Resilience,* Presidential Decision Directive 21, 2.

[78] Ibid., 3.

[79] Ibid., 4.

PPD 21 also required an update to the NIPP. The resulting work product was the NIPP 2013. This national plan embraces the collaborative process and was constructed with the active participation from the CI community and government representatives. The national plan focuses on “risk management” as the skeletal framework for CI “security and resilience” and encourages continued focus on stakeholder collaboration as a vital component of the risk management process.[80] The intended audience for this national plan includes, “wide-ranging critical infrastructure community comprised of public and private critical infrastructure owners and operators; Federal departments and agencies, including Sector–Specific Agencies (SSAs); State, local, tribal and territorial (SLTT) governments; regional entities; and other private and non-profit organizations charged with securing and strengthening the resilience of critical infrastructure.”[81]

The National Plan illustrates that mitigating CI vulnerability requires a unified strategy, joining the broad private and government sectors, to accomplish three key objectives.[82] The first key objective of the National Plan is to, “identify, deter, detect, disrupt and prepare for threats and hazards to the nation’s critical infrastructure.” The second key objective is to, “reduce vulnerabilities of critical assets, systems and networks.” The final objective of the National Plan is to, “mitigate the potential consequences to critical infrastructure of incidents or adverse actions that do occur.”

The National Plan designs a, “national unity of effort to achieve critical infrastructure security and resilience.”[83] The core of the National Plan is the “call to action” section, which “guides efforts to achieve national goals aimed at enhancing national critical infrastructure security and resilience,” collaboratively

---

[80] U.S. Department of Homeland Security, *NIPP 2013: Partnering for Critical Infrastructure Security and Resilience* (Washington, DC: U.S. Department of Homeland Security, 2013), 4.

[81] Ibid., 3.

[82] Ibid.

[83] Ibid., 2.

within the critical infrastructure community.[84] The 12 specific calls to action are broken down into three categories.

The first category within this call to action is, “Build upon Partnership Efforts,” and contains four specific calls to action.[85] The first call to action for this category is to, “set a national focus through jointly developed priorities.” The second call to action in this category is to, “determine collective actions through joint planning efforts.” The third call to action for the category is to, “empower local and regional partnerships to build capacity nationally.” The final categorical call to action is to, “leverage incentives to advance security and resilience.”

The second category within the call to action section is, “innovate in managing risk,” and contains six specific calls to action.[86] The first call to action for this category is, “enable risk informed decision making through enhanced situational awareness.” The second call is, “analyze infrastructure dependencies, interdependencies and associated cascading effects.” The third call is, “identify, assess and respond to unanticipated infrastructure cascading effects during and following incidents.” The fourth call is to “promote infrastructure, community and regional recovery following incidents.” The fifth call is to “strengthen coordinated development and delivery of technical assistance, training and education.” The final call is to, “improve critical infrastructure security and resilience by advancing research and development solutions.”

The third and final category is, “focus on outcomes,” and contains two specific calls to action.[87] The first call to action for this category is to, “evaluate progress toward the achievement of goals.” The second call is to, “learn and adapt during and after exercises and incidents.”

---

[84] U.S. Department of Homeland Security, *NIPP 2013: Partnering for Critical Infrastructure Security and Resilience*, 2.

[85] Ibid., 21.

[86] Ibid.

[87] Ibid.

C. NATIONAL CYBERSECURITY FRAMEWORK

EO 13636 required the implementation of a "voluntary and risk based" "Cybersecurity Framework."[88] The objective of the Framework was the collaborative development of, "a set of industry standards and best practices to help organizations manage cybersecurity risks."[89] NIST presented the resulting framework in February 2014.[90] The report notes, "use of this voluntary framework is the next step to improve the cybersecurity of our nation's critical infrastructure—providing guidance for individual organizations, while increasing the cybersecurity posture of the nation's critical infrastructure as a whole."[91] The "Cybersecurity Framework" is composed of three parts.

The framework core is the first part. It is a set of, "cybersecurity activities, desired outcomes, and applicable references that are common across critical infrastructure sectors."[92] This framework core is comprised of five primary functions: "identify, protect, detect, respond, and recover."[93] The core facilitates the dissemination of cyber security information throughout organizations from senior executives all the way down to line level employees.[94] It also provides basic steps an organization can take to facilitate working toward specific cyber security goals, which will assist its organization with mitigating cyber security vulnerabilities.[95]

The framework implementation tiers, "provide context on how an organization handles cybersecurity risk and the processes in place to manage

---

[88] National Institute of Standards and Technology, *Framework for Improving Critical Infrastructure Cyber Security*, 1.

[89] Ibid.

[90] Ibid.

[91] Ibid.

[92] Ibid., 4.

[93] Ibid.

[94] Ibid.

[95] Ibid., 7.

that risk."[96] The tiers are used to specify the level at which an organization has adopted and implemented outlined cyber security vulnerability mitigation practices and their adherence to the standards defined within the "cybersecurity framework." The designation process of tiers, "considers an organization's current risk management practices, threat environment, legal and regulatory requirements, business/mission objectives, and organizational constraints."[97] The tiers categorize an organization's procedures through a continuum describing increasing sophistication of practices from partial (tier 1), to risk informed (tier 2), to repeatable (tier 3), to adaptive (tier 4).[98]

The framework profile is characterized as the, "alignment of standards, guidelines, and practices to the framework core in a particular implementation scenario."[99] The profiles are designed to highlight cyber security weakness and improve cyber security preparedness, through the comparison of a current performance standard profile with a desired performance profile standard, to identify vulnerabilities for mitigation.[100]

The Framework can be used as a tool to manage cybersecurity risk by identifying the key operational functions in need of attention and then prioritizing spending to address these deficiencies.[101] The Framework is intended to complement, not replace, an organization's existing cybersecurity program.[102] However, if an organization does not have a current program, the Framework can serve as the foundation for the development of a brand new cyber security program.[103] Lastly, the Framework develops, "a common language to

---

[96] National Institute of Standards and Technology, *Framework for Improving Critical Infrastructure Cyber Security*, 5.

[97] Ibid., 9.

[98] Ibid.

[99] Ibid., 5.

[100] Ibid., 11.

[101] Ibid., 13.

[102] Ibid.

[103] Ibid.

communicate among interdependent stakeholders" who are responsible for protecting CI services.[104]

U.S. CI cybersecurity policy has evolved greatly over the past two decades. The complex policy is an interwoven fabric containing a combination of varied types of national policy documents. The policy has evolved from an initial focus on physical security to an intense focus on cybersecurity. The policy has evolved from a baseline of definitions and sector identifications all the way to the National Cybersecurity Framework for CI Protection and the National Infrastructure Protection Plan. Some of the policies are classified documents permitting cyber defenses that cannot be detailed, and other policies are open source documents crafted with the inclusion of the public sector in mind. One thing is clear, as technology evolves, so must this nation's policies and focus on cyber security.

[104] National Institute of Standards and Technology, *Framework for Improving Critical Infrastructure Cyber Security*, 15.

THIS PAGE INTENTIONALLY LEFT BLANK

III. U.S. CRITICAL INFRASTRUCTURE AND ICS

U.S. national well-being and the fabric American's daily lives rely upon the security and resiliency of U.S. CIs. The DHS refers to CI as the, "backbone of our nation's economy, security and health."[105] Although it is most often taken for granted, CI unknowingly touches everyone's daily lives when using electricity, consuming clean water, utilizing mass transportation, and communicating via cell phones or computers.[106] The CI systems and facilities that provide these foundational services have become increasingly computer reliant and networked. Computerized components, called ICS, measure and control many of the industrial or mechanical processes needed to produce the desired outputs of this nation's CIs.

A. CI DEPENDENCY ON ICS COMPUTER TECHNOLOGY

Computerized ICS are vital components in U.S. CI industries. They facilitate the ability to manage multiple sites or processes from a single control center.[107] The networking of separate ICS has made it possible to achieve extraordinary efficiency thanks to the management of real time system information during industrial processes.[108]

ICS facilitate the management and regulation of the generation, transmission, and distribution of electricity.[109] It is accomplished for example by, "opening and closing circuit breakers and setting thresholds for preventive

---

105 "What Is Critical Infrastructure."

106 Ibid.

107 Dana A. Shea, *Critical Infrastructure: Control Systems and the Terrorist Threat* (CRS Report No. RL31534) (Washington, DC: Congressional Research Service, 2004), 3, http://fas.org/irp/crs/RL31534.pdf.

108 Ibid.

109 Gheorghe Boaru and George-Ionut Badita, "Critical Infrastructure Protection Challenges and Efforts to Secure Control Systems," Romanian National Defense University, Regional Department of Defense Resources Management Studies, 2008, 148, http://search.proquest.com/docview/1136853092?accountid=12702.

shutdowns."[110] The electric and gas industry controls refinery operations by using integrated ICS to, "remotely monitor the pressure and flow of gas pipelines, and control the flow and pathways of gas transmission."[111]

Water utilities monitor well levels, control pumps, and water flows, and measure tank levels or pressure, remotely with ICS.[112] They also remotely monitor water quality characteristics, such as pH, turbidity and chlorine levels, and even control the addition of chemicals with ICS.[113] The enhanced productivity facilitated by ICS has led to greater reliance on these computerized systems to maximize the efficiency and output from U.S. CIs.

B. OVERVIEW OF INDUSTRIAL CONTROL SYSTEMS IN CI

ICS are computerized components, which are often networked, that control industrial processes through four basic steps. The first step is taking the accurate **measurement** of the status or condition of a process. The second step involves a controller **evaluating** potential actions to affect the process after considering that measurement and comparing it to the system's programmed optimal functioning values. The third step is the controller **sending** an output signal to alter the process based on the controller's evaluation of the measurement. The resulting fourth and final step is the reaction to that output signal that **manipulates** the process itself toward optimal efficiency.[114]

CI ICS may be classified within one of three common and widely used categories. The three primary categories are programmable logic computers

[110] Boaru and Badita, "Critical Infrastructure Protection Challenges and Efforts to Secure Control Systems," 149.

[111] Ibid.

[112] Ibid.

[113] Ibid.

[114] Tarun Agarwal, "A Glance on Industrial Control Systems with Control Strategies," EDGEFX.US, August 26, 2014, http://www.efxkits.us/industrial-control-systems-and-control-strategies/.

(PLCs), distributed control systems (DCSs) and supervisory control and data acquisition (SCADA)[115] systems.

Small computers called PLCs are used to control the automation of many electromechanical processes, such as the movement of machinery along an assembly line.[116] PLCs were first developed to aid in the mechanization of the automotive manufacturing industry. General Motors integrated the first PLCs into assembly lines in 1968 to replace hard-wired controller systems.[117] Since that time, PLCs have contributed greatly to the development and optimization of factory automation.[118]

PLCs have a programmable memory for storing instructions needed to carry out specific industrial functions.[119] Some of those functions include logic, timing, counting communication, arithmetic, and data processing.[120] The output of the PLC may include regulating functions, such as operational control of automobile assembly line processes, and power plant soot blowers.[121] PLCs are often networked with both SCADA and DCS technologies as, "control components of hierarchical systems to provide local management of processes through feedback control."[122]

DCSs are specially designed ICS used to control complex and distributed applications within a facility.[123] DCS controller components are distributed throughout an entire plant area but within the same geographic location.[124]

---

115 Agarwal, "A Glance on Industrial Control Systems with Control Strategies."

116 "What Is a Programmable Logic Controller (PLC)?," accessed June 20, 2015, http://www.wisegeek.org/what-is-a-programmable-logic-controller.htm.

117 Ibid.

118 Ibid.

119 Stouffer et al., *Guide to Industrial Control Systems Security*, 2–12.

120 Ibid.

121 Ibid.

122 Ibid.

123 Agarwal, "A Glance on Industrial Control Systems with Control Strategies."

124 Ibid.

These systems maintain supervisory control over multiple integrated systems responsible for localized industrial processes and are programmed to maintain process conditions around a desired set point.[125] In current systems, DCSs may be incorporated with business computer networks to provide management with a real time view of plant operations.[126] Some examples of CIs that use DCS technology during production include "oil refineries, water and wastewater treatment, electric power generation plants, chemical manufacturing plants, automotive production, and pharmaceutical processing facilities."[127]

SCADA systems are advanced ICS specifically designed to collect field data from instruments at dispersed field sites and then process that field data at a central computer facility.[128] SCADA systems are the nerves transmitting signals and the brains processing those signals for many CI systems.[129] SCADA systems merge the ability to monitor remote location physical sites, relay human initiated commands to those remote physical sites, and even take autonomous action to control industrial processes based on field device readings and established algorithms.[130] These systemic reactions take place at near real time speed with a delay of only microseconds.[131] SCADA systems are the primary conduits for the raw data readings transmitted to a control center and the resulting returning commands to alter the industrial processes back from the control center.[132]

SCADA systems have become increasingly sophisticated and allow for the optimal operation of almost any process, automation, or manufacturing

---

[125] Stouffer et al., *Guide to Industrial Control Systems Security*, 2–10.

[126] Ibid., 2–12.

[127] Ibid.

[128] Ibid., 2–5.

[129] Morgan Henrie, "Cyber Security Risk Management in the SCADA Critical Infrastructure Environment," *Engineering Management Journal* 25, no. 2 (June 2013): 40, http://search.proquest.com/docview/1434438191?accountid=12702.

[130] Ibid.

[131] Ibid.

[132] Shea, *Critical Infrastructure: Control Systems and the Terrorist Threat*, 2.

system.[133] As a result, many CIs now operate at a level of safety, reliability, and efficiency that had never been achievable in the past.[134] SCADA systems facilitate operations in diverse CI distribution networks, such as water distribution systems, wastewater collection systems, oil and natural gas pipelines, electrical utility transmission systems, rail, and other public transportation systems.[135]

C. CI STAKEHOLDER IDENTIFICATION

The GAO reports that 85% of this nation's CI is privately owned.[136] Privately owned infrastructures include diverse properties, such as chemical plants, museums, casinos, hotels, conference centers, amusement parks, real estate, shopping centers, cell towers, Internet infrastructure, manufacturing facilities, dams, energy infrastructure, banks, farms, food processing facilities, hospitals, nuclear reactors, transportation carriers, and water treatment facilities.

Government owned infrastructures include assets, such as military bases and facilities, defense industry production plants, public emergency services (police, fire and emergency medical), government owned utilities and government owned and controlled physical facilities. With this ownership diversity in mind, the DHS notes, "Ensuring the protection and resilience of the nation's critical infrastructure is a shared responsibility among multiple stakeholders—neither government nor the private sector alone has the knowledge, authority, or resources to do it alone."[137] The interdependency of U.S. CIs cannot be overstated. Even exclusively government owned CI, such as a military base or

---

[133] Henrie, "Cyber Security Risk Management in the SCADA Critical Infrastructure Environment," 40.

[134] Ibid.

[135] Stouffer et al., *Guide to Industrial Control Systems Security*, 2–5.

[136] U.S. Government Accountability Office, *Critical Infrastructure Protection—Progress Coordinating Government and Private Sector Efforts Varies by Sectors' Characteristics* (GAO-07-39) (Washington, DC: U.S. Government Accountability Office, 2006), 1, http://www.gao.gov/new.items/d0739.pdf.

[137] "Critical Infrastructure Protection Partnerships and Information Sharing," last modified April 14, 2015, http://www.dhs.gov/critical-infrastructure-protection-partnerships-and-information-sharing.

government building, are dependent upon private sector CI for services, such as electricity, water services, and communications.

D. CRITICAL INFRASTRUCTURE SECTORS IN THE UNITED STATES

CI is defined in the National Infrastructure Protection Plan 2013 as the, "systems and assets, whether physical or virtual, so vital to the United States that the incapacity or destruction of such systems and assets would have a debilitating impact on security, national economic security, national public health or safety, or any combination of those matters."[138] PPD 21 identifies a total of 16 separate CI sectors. Categorizing U.S. CI into sectors is the best way to evaluate them because each sector has unique characteristics, regulatory environments, operating intricacies, and risk profiles.[139] The DHS breaks down U.S. CI into the following 16 sectors.

The "chemical sector" is a vital element of the U.S. economy.[140] It is interdependent with many other other CI sectors, and carries notable public safety implications due to hazards present in production processes. Much of the chemical sector is comprised of private sector entities, which necessitates collaboration between the DHS and private industry on security and resilience initiatives.[141]

Structures within the "commercial facilities sector," "operate on the principle of open public access, meaning that the general public can move freely throughout these facilities without the deterrent of highly visible security barriers."[142] Private sector ownership is common throughout this sector and little,

---

[138] U.S. Department of Homeland Security, *NIPP 2013: Partnering for Critical Infrastructure Security and Resilience*, 29.

[139] The White House Office of the Press Secretary, *Critical Infrastructure Security and Resilience,* Presidential Decision Directive 21, 6, Washington, DC: The White House Office of the Press Secretary, 2013.

[140] "Chemical Sector," last modified July 16, 2015, http://www.dhs.gov/chemical-sector.

[141] Ibid.

[142] "Commercial Facilities Sector," last modified August 27, 2014, http://www.dhs.gov/chemical-sector.

if any, government regulation or interaction occurs with facility operators.[143] Some of the building types included within the sector include stadiums, museums, casinos, hotels, conference centers, amusement parks, movie theatres, broadcast media studios, office buildings, condominium, or apartment buildings and shopping malls.[144]

According to the DHS, the "communications sector" is, "an integral component of the U.S. economy, underlying the operations of all businesses, public safety organizations, and government."[145] It is identified as a particularly critical sector due to its role as a vital bridge between all CI sectors. The DHS notes the provision of these services, "has become interconnected; satellite, wireless, and wire line providers depend on each other to carry and terminate their traffic and companies routinely share facilities and technology to ensure interoperability."[146] The private sector owns and operates the majority of communications infrastructure. These stakeholders are primarily responsible for protecting the infrastructure, but work with the federal government on security and resilience initiatives.[147]

The "critical manufacturing sector" is yet another sector with key implications for the health of the U.S. economy.[148] According to the DHS, "A direct attack on or disruption of key elements of the manufacturing industry could disrupt essential functions at the national level and across multiple critical infrastructure sectors."[149] The critical manufacturing sector includes four central industries as the sector's foundation that includes "primary metal manufacturing; machinery manufacturing; electrical equipment, appliance, and component

143 "Commercial Facilities Sector."

144 Ibid.

145 Ibid.

146 Ibid.

147 Ibid.

148 "Critical Manufacturing Sector," last modified December 4, 2014, http://www.dhs.gov/critical-manufacturing-sector.

149 Ibid.

manufacturing; and transportation equipment manufacturing."[150] The bulk of the critical manufacturing sector is controlled by the private sector.

According to the DHS, the "dams sector," "delivers critical water retention and control services in the United States, including hydroelectric power generation, municipal and industrial water supplies, agricultural irrigation, sediment and flood control, river navigation for inland bulk shipping, industrial waste management, and recreation."[151] The sector is comprised of assets, such as "dam projects, hydropower generation facilities, navigation locks, levees, dikes, hurricane barriers, mine tailings, other industrial waste impoundments, and other similar water retention and water control facilities."[152] The dams sector shares interdependencies with many other sectors and contains over 87,000 dams, of which roughly 65% share private ownership.[153]

The "Defense Industrial Base Sector is the worldwide industrial complex that enables research and development, as well as design, production, delivery, and maintenance of military weapons systems, subsystems, and components or parts, to meet U.S. military requirements."[154] The DHS reports that the, "Defense Industrial Base partnership consists of Department of Defense components, more than 100,000 Defense Industrial Base companies and their subcontractors who perform under contract to the Department of Defense, companies providing incidental materials and services to the Department of Defense, and government-owned/contractor-operated and government-owned/government-operated facilities."[155] Simply put, this sector provides the many goods and services needed to conduct the military operations vital to defending U.S. interests.[156]

---

150 "Critical Manufacturing Sector."

151 "Dams Sector," last modified December 11, 2014, http://www.dhs.gov/dams-sector.

152 Ibid.

153 Ibid.

154 "Defense Industrial Base Sector," last modified June 12, 2014, http://www.dhs.gov/defense-industrial-base-sector.

155 Ibid.

156 Ibid.

The DHS defines the “emergency services sector” as, “Our system of prevention, preparedness, response, and recovery elements that represent the nation’s first line of defense in the prevention and mitigation of risk from both intentional and unintentional manmade incidents, as well as from natural disasters.”[157] The emergency services sector also defends the other 15 critical infrastructure sectors, which makes them all highly interdependent on this sector. emergency services sector assistance is provided primarily by state and local government agencies. The sector is built on the foundation of five primary disciplines to include “law enforcement; fire and emergency services; emergency management; emergency medical services and public works.”[158]

“Energy sector” infrastructure powers this nation’s economy. According to the DHS, “without a reliable energy supply, health and welfare are threatened, and the U.S. economy cannot function.”[159] Societal reliance on electricity means that all sectors share dependence on the energy sector.[160] The DHS subdivides the energy sector into “three interrelated segments,” including “electricity, petroleum, and natural gas.”[161] Over 80% of U.S. “energy sector” infrastructure is privately owned, and provides energy to the “transportation systems sector,” power to homes and commercial properties, and alternative energy products essential to powering society.[162] This high percentage blend of private ownership within this critical sector requires the DHS to collaborate with key sector partners on security and resilience initiatives.

The “financial services sector” plays a vital role in almost every other CI sector within the United States. The banking industry is collated and regulated based on the differing types of programs and products that banks provide to

---

157 “Defense Industrial Base Sector.”

158 Ibid.

159 “Energy Sector,” last modified June 17, 2015, http://www.dhs.gov/energy-sector.

160 Ibid.

161 Ibid.

162 Ibid.

customers.[163] Institutions offer a wide array of programs and fluctuate widely in size from small community credit unions all the way up to established international banks with portfolios worth over a trillion dollars.[164] According to the DHS, the sector contains, "more than 18,800 federally insured depository institutions" and "thousands of providers of various investment products."[165]

The DHS reports that the "food and agriculture sector" is, "almost entirely under private ownership and is comprised of an estimated 2.2 million farms, 900,000 restaurants, and more than 400,000 registered food manufacturing, processing, and storage facilities."[166] The DHS adds that this sector is responsible for approximately 20% of overall U.S. financial activity and is interdependent with a number of other sectors, as it provides nourishment to those working in all of this country's CI sectors.[167]

The DHS points out that the "government facilities sector" includes a diverse range of structures, located both domestically and outside U.S. borders, which are controlled by "federal, state, local, and tribal governments."[168] The DHS notes further, "these facilities include general-use office buildings and special-use military installations, embassies, courthouses, national laboratories, and structures that may house critical equipment, systems, networks, and functions."[169] Along with buildings, the sector contains cyber components that, "contribute to the protection of sector assets (e.g., access control systems and

---

[163] "Financial Services Sector," last modified June 12, 2014, http://www.dhs.gov/financial-services-sector.

[164] Ibid.

[165] Ibid.

[166] "Food and Agriculture Sector," last modified June 12, 2014, http://www.dhs.gov/food-and-agriculture-sector.

[167] Ibid.

[168] "Government Facilities Sector," last modified June 12, 2014, http://www.dhs.gov/government-facilities-sector.

[169] Ibid.

closed-circuit television systems) as well as individuals who perform essential functions or possess tactical, operational, or strategic knowledge."[170]

The DHS considers the "healthcare and public health sector" as vital, for its role in shielding the vulnerable U.S. economy from "hazards such as terrorism, infectious disease outbreaks, and natural disasters."[171] This sector also plays a critical role in mitigation, response, and recovery efforts during disaster responses. The DHS goes on to note that, "while healthcare tends to be delivered and managed locally, the public health component of the sector, focused primarily on population health, is managed across all levels of government: national, state, regional, local, tribal, and territorial."[172] The bulk of the "healthcare and public health sector" is controlled privately, so partnerships and intelligence exchanges between the government and private sectors are crucial to expanding resilience within this sector.[173]

Due to societal reliance on digital communications technology, the DHS has identified the "information technology sector" as the foundation of, "the nation's security, economy, public health and safety."[174] The DHS goes on to note, "businesses, governments, academia, and private citizens are increasingly dependent upon Information Technology Sector functions." This sector's operations yield the "hardware, software, information technology systems" and services people need to interact with the Internet.[175] The functions of the IT sector are accomplished through a diverse network of primarily privately owned companies.[176]

---

[170] "Government Facilities Sector."

[171] "Health and Public Health Sector," last modified June 12, 2014, http://www.dhs.gov/healthcare-and-public-health-sector.

[172] Ibid.

[173] Ibid.

[174] "Information Technology Sector," last modified June 12, 2014, http://www.dhs.gov/information-technology-sector.

[175] Ibid.

[176] Ibid.

The DHS identifies the “nuclear reactors, materials and waste sector” as being inclusive of “nuclear power plants; non-nuclear reactors used for research, testing and training; manufacturers of nuclear reactors or components; radioactive materials used primarily in medical, industrial, and academic settings; nuclear fuel cycle facilities; decommissioned nuclear power reactors; and transportation, storage and disposal of nuclear and radioactive waste.”[177] Approximately one fifth of the electricity produced in the United States is generated through nuclear power. The DHS reports that there are, “100 commercial nuclear reactors licensed to operate at 62 nuclear power plants.”[178] The potentially devastating consequences of sabotage or attacks in this sector make it an intense national security focal point.

The U.S. “transportation systems sector” is responsible for the movement of cargo and passengers both domestically and internationally.[179] Within this sector, the DHS identifies “seven key subsectors, or modes to include: aviation; highway infrastructure and motor carrier; maritime transportation system; mass transit and passenger rail; pipeline systems; freight rail; and postal and shipping.”[180] This diverse and far-reaching sector is comprised of both government controlled and private sector owned components. The transportation systems sector is interdependent and intertwined with most of the other CI sectors.

The “water and wastewater systems sector” is comprised of entities that provide clean drinking water delivery and wastewater disposal services to the U.S. population. The DHS reports, “There are approximately 160,000 public drinking water systems and more than 16,000 publicly owned wastewater

177 “Nuclear Reactors, Materials and Waste Sector,” last modified November 24, 2014, http://www.dhs.gov/nuclear-reactors-materials-and-waste-sector.

178 Ibid.

179 “Transportation Systems Sector,” last modified March 25, 2013, http://www.dhs.gov/transportation-systems-sector.

180 Ibid.

treatment systems in the United States."[181] In addition, the DHS determined, "approximately 84 percent of the U.S. population receives their potable water from these drinking water systems, and more than 75 percent of the U.S. population has its sanitary sewerage treated by these wastewater systems."[182] Contaminated drinking water would constitute a real threat to the health and welfare of any affected population base in this country.

E. CI ICS VULNERABILITIES

Many of today's CI linked ICS evolved from the networking of IT capability into existing physical systems that replaced or supplemented physical control mechanisms.[183] Early ICS CI integrations were only susceptible "to local threats because their components were physically secured and were not connected" to company computer networks.[184] However, the trend toward integrating ICS with IT networks and online services provides less isolation and greater exposure to external threats for these systems. Existing ICS were not necessarily designed to withstand recently developed cyber threats.[185] Additionally, the prevalence of wireless networks places ICS at greater risk from hackers who only need to be relatively close in physical proximity, but do not need actual physical access to the equipment.[186] Subsequently, early ICS, linked to corporate computer systems, are vulnerable to cyber attacks initiated through both wireless signals and the Internet.[187]

---

[181] "Water and Wastewater Systems Sector," last modified June 12, 2014, http://www.dhs.gov/water-and-wastewater-systems-sector.

[182] Ibid.

[183] Stouffer et al., *Guide to Industrial Control Systems Security*, 2–1.

[184] Ibid., 1.

[185] Nasser Abouzakhar, "Critical Infrastructure Cybersecurity: A Review of Recent Threats and Violations," *University of Hertfordshire School of Computer Science, Academic Conferences International Limited*, 2013, 1, http://search.proquest.com/docview/1400694816?accountid=12702.

[186] Stouffer et al., *Guide to Industrial Control Systems Security*, 1.

[187] Shea, *Critical Infrastructure: Control Systems and the Terrorist Threat*, 3.

According to the NIST, threats to CI ICS arise from numerous potential adversaries including "hostile governments, terrorist groups, disgruntled employees, malicious intruders, complexities, accidents and natural disasters."[188] Potential manipulative incidents affecting CI ICS may be initiated through at least five potential attack vectors. One attack vector noted by NIST would be a disruption of system information or command transmission, within ICS networks, that would potentially affect safe CI plant operations. A second vector highlighted by NIST would be, "unauthorized changes to instructions, commands, or alarm thresholds. This could damage, disable, or shut down equipment, create environmental impacts and endanger human life."[189] Misleading or false data transmitted to plant operations personnel is a third potential vector. NIST indicates such data could either cloak unauthorized system modulations or trigger operators to make ill-advised decisions on system operations, which may adversely impact CI facility operations. The modification of ICS software, configuration settings or malware infection is the fourth vector of concern noted by NIST that could have a number of negative side effects. Lastly, tampering with the processes of safety systems could put safety and lives at risk.[190]

Boaru and Badita, of the Romanian National Defense University, reveal four factors that contribute to the escalated modern threat posture for ICS. The first factor is the widespread adoption of standardized technology with known vulnerabilities.[191] Early implementations of ICS utilized proprietary, "hardware, software and network protocols," which complicate understanding how specific ICS work and make them difficult to hack.[192] It was a positive attribute from a security perspective. However, to cut costs and enhance productivity, companies

---

[188] Stouffer et al., *Guide to Industrial Control Systems Security*, 1.

[189] Ibid., 2.

[190] Ibid.

[191] Boaru, and Badita, "Critical Infrastructure Protection Challenges and Efforts to Secure Control Systems," 152.

[192] Ibid.

have been replacing older legacy ICS with cheaper common technologies.[193] These common technology systems unfortunately also carry common vulnerabilities, for which current malware already exists within the hacker community. As a result, a higher number of hackers have the skills required to initiate cyber attacks and a higher number of vulnerable ICS.[194]

Boaru and Badita's second noted factor, contributing to the escalated threat posture for ICS, is the network connectivity of ICS to other networks.[195] Companies frequently integrate their ICS with their corporate computer networks for business monitoring efficiency purposes. Some enterprises take this step further and connect their networks to those of strategic business partners and/or the Internet.[196] In addition, many ICS make use of; "wide area networks, and the Internet, to transmit data and commands to dispersed stations and individual devices."[197] The merging of ICS networks with "public and enterprise networks" opens these systems to ICS security vulnerabilities.[198] Absent appropriately robust security controls for both "the enterprise network and the ICS network," a breach in the "enterprise network" can adversely impact ICS functions.[199]

Boaru and Badita's third factor, contributing to the escalated threat posture for ICS, is the use of insecure remote connections.[200] Organizations often leave digital access ports open for remote access, diagnostics, and maintenance work on the system. Additionally, ICS that utilize wireless data transmission schemes

---

[193] Boaru, and Badita, "Critical Infrastructure Protection Challenges and Efforts to Secure Control Systems," 152.

[194] Ibid.

[195] Stouffer et al., *Guide to Industrial Control Systems Security*, 1.

[196] Boaru, and Badita, "Critical Infrastructure Protection Challenges and Efforts to Secure Control Systems," 152.

[197] Stouffer et al., *Guide to Industrial Control Systems Security*, 3–15.

[198] Boaru and Badita, "Critical Infrastructure Protection Challenges and Efforts to Secure Control Systems," 152.

[199] Ibid.

[200] Abouzakhar, "Critical Infrastructure Cybersecurity: A Review of Recent Threats and Violations," 4.

are particularly susceptible to cyber attacks.[201] Hackers can use these connections to remote into the system if it is not protected with authentication protocols or encryption.[202] Without these data safety measures, not much can be done to validate information traveling through unsecure wireless systems.

Boaru and Badita's fourth factor, contributing to the escalated threat posture for ICS, is the widespread distribution of technical information about ICS through the Internet.[203] Public information about ICS and CI is easily accessible to hackers and malicious actors on the web. This availability was highlighted by a graduate student from George Mason University, who in his dissertation, "mapped every business and industrial sector in the American economy to the fiber-optic network that connects them, using material that was available publicly on the Internet."[204] Public records and information is a double-edged sword, which unlocks both increased capacity for study and increased vulnerability to those planning attacks.

[201] Boaru and Badita, "Critical Infrastructure Protection Challenges and Efforts to Secure Control Systems," 153.

[202] Ibid.

[203] Stouffer et al., *Guide to Industrial Control Systems Security*, 3–16.

[204] Boaru and Badita, "Critical Infrastructure Protection Challenges and Efforts to Secure Control Systems," 153.

IV. STUXNET ATTACK CASE STUDY

In June 2012, the cyber security landscape changed when a Belarusian cyber security firm named "VirusBlokAda"[205] detected the presence of a new and sophisticated malware, later dubbed "Stuxnet," in the computers of an Iranian nuclear facility. Other technology security firms joined the intense investigation of this unclaimed malware and determined that the Stuxnet worm had been specifically engineered to infect specialized Siemens computer components that were designed to run centrifuges in Iran's Natanz nuclear facility.[206] This newly discovered malware surprised computer security specialists in that it sought no corporate or financial advantage like most malware of the era.[207] The code was programmed to control and destroy discreetly the centrifuge components of the Natanz nuclear facility.[208] Analysts logically concluded that Stuxnet was the first politically motivated cyber attack,[209] and it showed that such an attack could cause significant physical damage to a CI facility.[210]

A. WHAT IS STUXNET?

Stuxnet was a "cyber-physical" attack, which means that the code actually caused real world physical damage, which requires interaction with three different CI layers and their specific vulnerabilities.[211] The IT layer is exploited to spread the malware, the ICS layer is exploited to manipulate process control, and the physical layer is where the resulting damage is developed.[212] The ultimate goal of Stuxnet was to sabotage Iran's uranium enrichment facility by

---

205 Nakashima, "Stuxnet Malware Is Blueprint for Computer Attacks on U.S."

206 Kushner, "The Real Story of Stuxnet,"

207 Ibid.

208 Warrick, "Iran's Natanz Nuclear Facility Recovered Quickly from Stuxnet Cyberattack."

209 Kushner, "The Real Story of Stuxnet,"

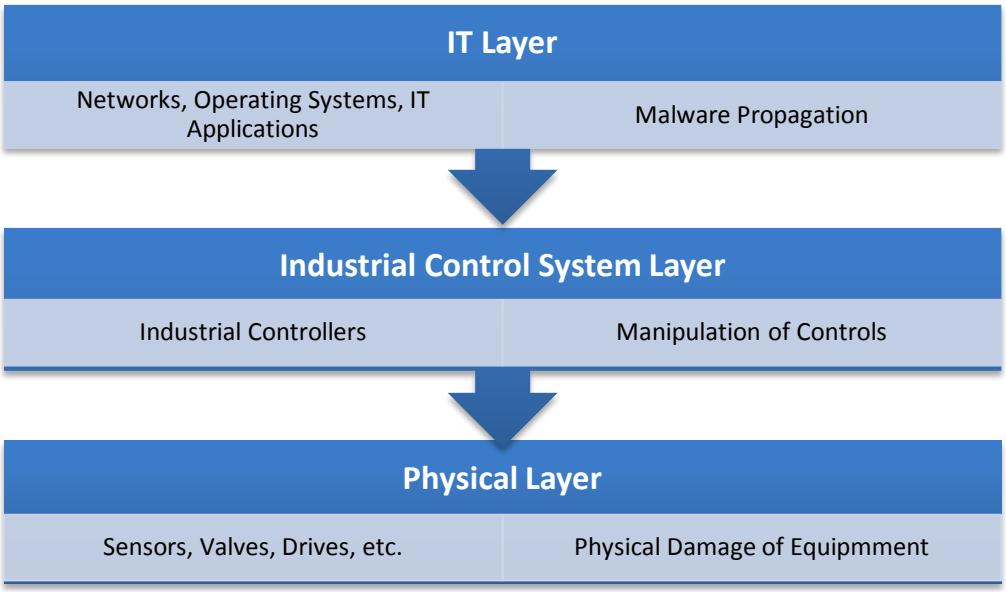
210 Kroft, "Stuxnet: Computer Worm Opens New Era of Warfare."

211 Langer, "To Kill a Centrifuge," 4.

212 Kroft, "Stuxnet: Computer Worm Opens New Era of Warfare."

reprogramming the PLCs controlling the fast spinning enrichment centrifuges, to ranges outside their specified boundaries, which would, in turn, damage the vulnerable centrifuge rotors.[213] The Stuxnet attack provides a textbook example of how the exploitation of these three layers can be leveraged to create physical destruction during a cyber attack.[214] See Figure 2.

Figure 2. Cyber Physical Attack Layers



Source: Ralph Langer, "To Kill a Centrifuge," The Langer Group, November 2013, 4, http://www.langner.com/en/wp-content/uploads/2013/11/to-kill-a-centrifuge.pdf.

Operationally, Stuxnet is classified as a complex computer worm.[215] Computer worms may be defined as, "malicious software applications designed to spread via computer networks."[216] Worms typically reside in a computer's

[213] Nicolas Falliere, Liam Murchu and Eric Chen, "W32.Stuxnet Dossier," Symantec, February 2011, 2, https://www.symantec.com/content/en/us/enterprise/media/security_response/whitepapers/w32_stuxnet_dossier.pdf.

[214] Langer, "To Kill a Centrifuge," 4.

[215] Karnouskos, "Stuxnet Worm Impact on Industrial Cyber-Physical System Security."

[216] Bradley Mitchell, "Computer Worm—Internet Security Terms," Compnetworking, accessed February, 3, 2015, http://compnetworking.about.com/cs/worldwideweb/g/bldef_worm.htm.

active memory and duplicate themselves. Worms use, "parts of an operating system that are automatic and are usually invisible to the user."[217] It is not uncommon for worms to go unnoticed until their replication depletes system memory to the point where it slows or modifies the computer's operations.[218] The 500-kilobyte Stuxnet worm was specifically programmed to infect the system components of Iran's high security Natanz uranium enrichment facility.[219]

B. GEOPOLITICAL FACTORS FRAMING THE STUXNET ATTACK

The Stuxnet attack should be viewed within the political context of the Iranian nuclear program. Iran was a ratifying signatory of the Nuclear Nonproliferation Treaty (NPT) in 1970 and completed their required International Atomic Energy Agency (IAEA) safeguards agreement in 1974.[220] Since that time, frequent and widespread concern has been raised that Iran has been seeking to develop nuclear weapons and has not lived up to the obligations of its commitment to the NPT. The controversy concerning Iranian nuclear weapons development programs began as early as 2002 when the IAEA began investigating allegations into clandestine nuclear activities in Iran.[221] The IAEA determined verifiable non-compliance issues were present and Iran has developed a combative posture with the international community and the IAEA since that time, as it pertains to nuclear NPT compliance.

In 2004, Iran began to experience a conservative political resurgence when conservatives regained control of the parliament in elections. This development was closely followed up with a hardline candidate, and Tehran mayor, Mahmoud Ahmadinejad, winning the presidential election in 2005, to

---

[217] Margaret Rouse, "Worm Definition," Tech Target Network, last accessed November 29, 2015, http://searchsecurity.techtarget.com/definition/worm.

[218] Ibid.

[219] Kushner, "The Real Story of Stuxnet."

[220] Paul K. Kerr, *Iran's Nuclear Program: Tehran's Compliance with International Obligations* (CRS Report No. R40094) (Washington, DC: Congressional Research Service, 2015), 1, fas.org/sgp/crs/nuke/R40094.pdf.

[221] Ibid., 4.

solidify conservative rule in Iran, which wrestled power away from reformist president Mohammad Khatami's government.[222] Ahmadinejad was quoted in 2005 as saying Israel should be "wiped off of the face of the world" and then announced in 2006 that Iran had successfully enriched uranium.[223] He also gained notoriety in 2005 for publicly denying the existence of the holocaust and calling the Nazi extermination campaign of Jews a "myth."[224] These developments occurred within the context of increasing Iranian tensions with both the U.N. and IAEA. It was the backdrop setting the stage for the development and deployment of the Stuxnet attack on Natanz.

C. WHAT MADE STUXNET UNIQUE

Stuxnet's production and implementation achieved several milestones in malware or malicious code history. It is the first to exploit four "zero-day" vulnerabilities.[225] A "zero day" refers to a vulnerability or exploitable gap in a computer program, which is unknown to the developer. Hackers may exploit this gap until the developer becomes aware and rushes to fix it with a security patch.[226] Stuxnet was also the first malware to compromise two digital certificates.[227] Digital certificates are, "trusted ID cards in electronic form that bind a website's public encryption key to their identity for purposes of public trust."[228] Digital certificates are, "issued by independent, recognized and mutually trusted third parties," which authenticate a website, and verify it is operating as

---

222 "Iran Profile—Timeline," July 14, 2015, http://www.bbc.com/news/world-middle-east-14542438.

223 Keith S. McLachlan, "Iran in 2006," *Encyclopedia Britannica*, accessed September 19, 2015, http://www.britannica.com/place/Iran-Year-In-Review-2006.

224 Bozorgmehr Sharafedin, "Why Iran Takes Issue with the Holocaust," *BBC News*, October 9, 2013, http://www.bbc.com/news/world-middle-east-24442723.

225 Falliere, Murchu and Chen, "W32.Stuxnet Dossier," 55.

226 Pctools, "What is a Zero Day Vulnerability?," Symantec, accessed September 19, 2015, http://www.pctools.com/security-news/zero-day-vulnerability/.

227 Falliere, Murchu, and Chen, "W32.Stuxnet Dossier," 55.

228 "What Are Digital Certificates?" http://www.wisegeek.com/what-are-digital-certificates.htm.

who it claims to be from a security standpoint.[229] Finally, Stuxnet injected code into ICS and both reprogrammed them and successfully hid it from the operators, to create physical damage to machinery.[230]

Stuxnet is a highly complex cyber weapon that required "nation-state" level resources for intelligence gathering, infiltration, and testing during its development.[231] Cyber security industry experts believe developers would have needed to setup a target mirrored testing environment that included the necessary ICS hardware, PLCs, modules, and peripheral equipment to test their code.[232] A fully functional mock uranium enrichment facility, replicating a top-secret plant, would be beyond the reach of organized crime rings or terrorist organizations.[233] However, Stuxnet has highlighted that successful cyber attacks on CI are possible. Less sophisticated, copycat style attacks of civilian CI targets could be made much easier utilizing the lessons learned from Stuxnet.[234]

In fact, similar malware agents have already been deployed on energy sector CI targets since the discovery of Stuxnet. "Havex" is a Stuxnet like malware agent designed to conduct industrial espionage of energy sector ICS. Like Stuxnet, Havex gathers information from the local network and reports back to a command and control server.[235] Havex was recently deployed to conduct industrial espionage on a number of European energy companies.[236] The DHS has identified a similar and sophisticated malware agent dubbed "Black Energy,"

---

[229] "What Are Digital Certificates?"

[230] Falliere, Murchu, and Chen, "W32.Stuxnet Dossier," 55.

[231] Langer, "To Kill a Centrifuge," 20.

[232] Falliere, Murchu and Chen, "W32.Stuxnet Dossier," 3.

[233] Langer, "To Kill a Centrifuge," 20.

[234] Ibid.

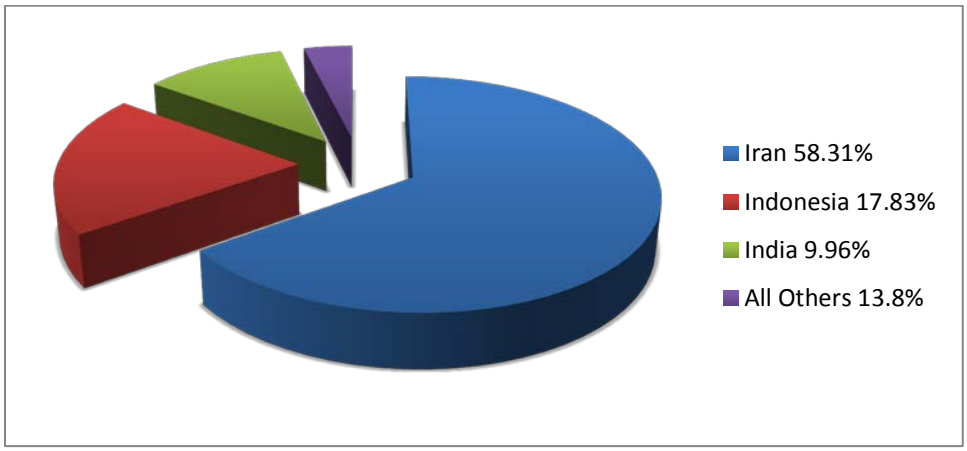
[235] Swati Khandelwal, "Stuxnet-like 'Havex' Malware Strikes European SCADA Systems," The Hacker News, June 26, 2014, http://thehackernews.com/2014/06/stuxnet-like-havex-malware-strikes.html.

[236] Ibid.

within the ICS of U.S. CI.[237] Although developers with significant engineering expertise designed Black Energy for industrial espionage, experts believe it could be weaponized to inject destructive code directly into ICS.[238]

In July 2010, Symantec deployed a strategy to analyze web data exchanges with the Stuxnet "command and control servers."[239] Symantec was provided with a vantage point to, "observe rates of infection and identify the locations of infected computers."[240] See Figure 3. Symantec's data identified approximately 100,000 infected hosts with just fewer than 60% being located in Iran.[241] This concentration of infections indicates that Iran was the initial target for infections with the other infections likely being "collateral damage."[242]

Figure 3. Global Distribution of Stuxnet Infections



Source: Nicolas Falliere, Liam Murchu, and Eric Chen, "W32.Stuxnet Dossier," Symantec, February 2011, 6, https://www.symantec.com/content/en/us/enterprise/media/security_response/whitepapers/w32_stuxnet_dossier.pdf.

[237] Aaron Ernst, "Is This the Future of Cyberwarfare?," AlJazeera America, February, 5, 2015, http://america.aljazeera.com/watch/shows/america-tonight/articles/2015/2/5/blackenergy-malware-cyberwarfare.html.

[238] Ibid.

[239] Falliere, Murchu, and Chen, "W32.Stuxnet Dossier," 5–6.

[240] Ibid.

[241] Ibid.

[242] Ibid., 7.

D. STUXNET FUNCTIONALITY AND PHASED DEPLOYMENT

Stuxnet was engineered to be hand carried into the Natanz plant to infect the computers. The Natanz computers were a closed system, absent Internet connectivity, which required Stuxnet to be physically introduced by a device, such as a corrupted removable drive.[243] Symantec experts believe, "this may have occurred by infecting a willing or unknowing third party, such as a contractor who perhaps had access to the facility, or an insider."[244] Once introduced to the facility, one of the primary propagation methods for Stuxnet was that it was designed to copy itself onto inserted removable drives each time one was used. This method exploited the closed system environment of Natanz where operators exchanged data with other computers by using removable drives.[245] Stuxnet also had the ability to replicate itself and spread once it infected a host computer with network access.[246]

Stuxnet is a sophisticated malware agent that was part of a multi-stage attack, which is outlined in Figure 4. The initial stage called for the development of computer code called a beacon that would be installed onto the computers at the facility.[247] The beacon created a network blueprint, or map of the Natanz plant, to detail how the computer systems controlled the centrifuges.[248] Duqu, a data-stealing piece of malware, is believed to be the reconnaissance agent used to map the Natanz computer network in 2007.[249] Once the mapping task was completed, the beacon covertly reported home on its work, through the Internet,

---

[243] Mark Hosenball, "Experts Say Iran Has Neutralized Stuxnet Virus," *Reuters*, February 14, 2012, http://www.reuters.com/article/2012/02/14/us-iran-usa-stuxnet-idUSTRE81D24Q20120214.

[244] Falliere, Murchu, and Chen, "W32.Stuxnet Dossier," 3.

[245] Ibid., 29.

[246] Ibid., 25.

[247] Sanger, "Obama Order Sped Up Wave of Cyberattacks Against Iran."

[248] Ibid.

[249] Jim Finkle, "Factbox: Cyber Warfare Expert's Timeline for Iran Attack," Reuters, December 2, 2011, http://www.reuters.com/article/2011/12/02/us-cyberattack-iran-idUSTRE7B10AV20111202.

using the networked computers to which it had spread.[250] This covert data transmission, sent back to the Stuxnet command and control servers in Malaysia and Denmark, was facilitated through two bogus websites set up cleverly to disguise the web traffic as legitimate soccer fan activity through "mypremierfutbol.com" and "todaysfutbol.com."[251]

The payload portion of the Stuxnet worm was then injected into Natanz and covertly worked its way through the computer network to the targeted and pre-designated PLCs.[252] During this next stage of the attack, the Stuxnet worm modified the code running the facility's PLCs to change their programmed operations.[253] These PLCs controlled the precise speed needed to spin the centrifuges used for uranium enrichment properly. Stuxnet caused the centrifuges to spin off speed and out of control, while at the same time, reporting false data to the operators that operations were progressing normally.[254]

Rotor wall pressure is a vulnerability for centrifuges and its control is a function of process pressure and rotor speed.[255] The easiest way to increase rotor wall pressure, and system stress, is to speed up the rotors. Stuxnet reprogrammed the PLCs that spun the centrifuges at 63,000 rpm, to speed them up by one-third, to 84,600 rpm for periods of 15 minutes at a time.[256] This increase led to the premature degradation and destruction of centrifuge components, delays in enrichment activities, and baffled scientists at the plant

[250] Sanger, "Obama Order Sped Up Wave of Cyberattacks against Iran."

[251] Falliere, Murchu, and Chen, "W32.Stuxnet Dossier," 21.

[252] Kroft, "Stuxnet: Computer Worm Opens New Era of Warfare.

[253] Karnouskos, "Stuxnet Worm Impact on Industrial Cyber-Physical System Security."

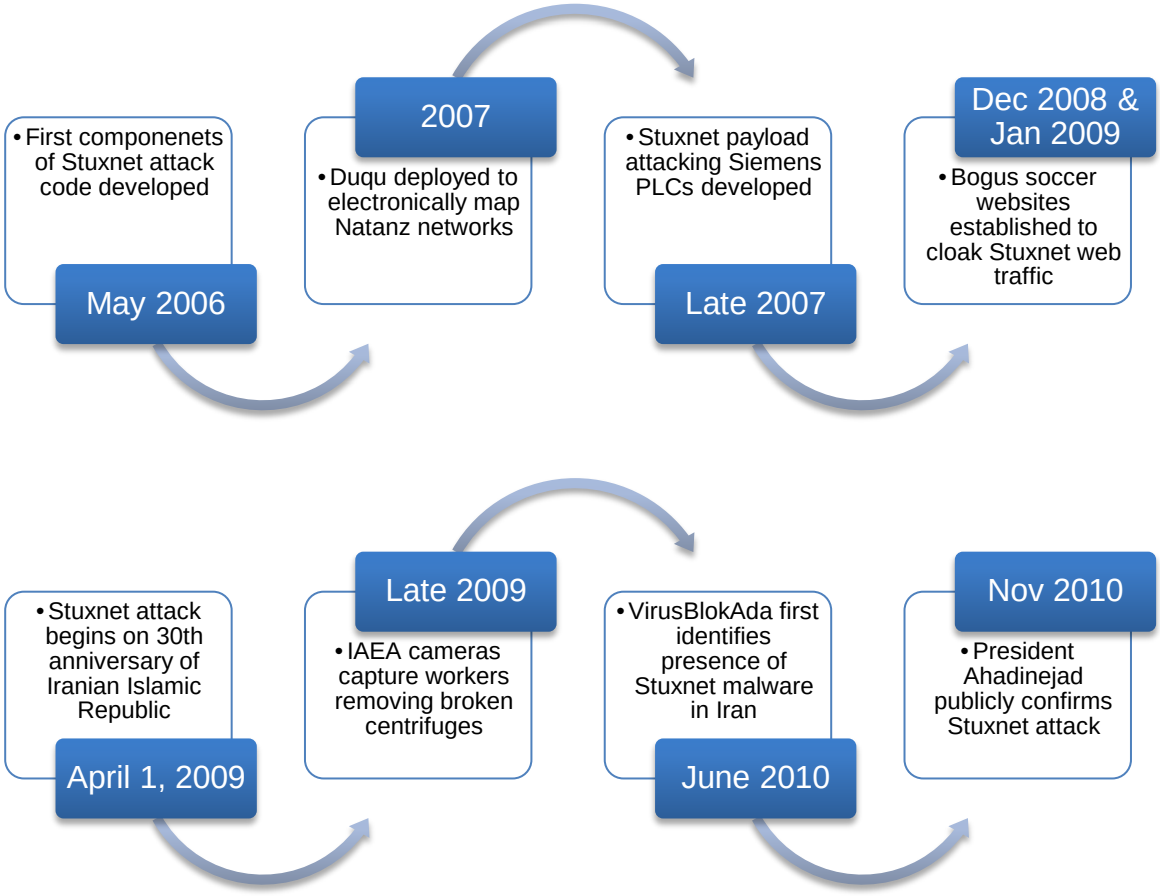
[254] Sanger, "Obama Order Sped Up Wave of Cyberattacks against Iran."

[255] Langer, "To Kill a Centrifuge," 17.

[256] Ibid.

who began to look incompetent as a result of the recurring and unexplained damage.[257]

Figure 4. Stuxnet Phased Deployment Timeline



Source: Jim Finkle, "Factbox: Cyber Warfare Expert's Timeline for Iran Attack," *Reuters*, December 2, 2011, http://www.reuters.com/article/2011/12/02/us-cyber attack-iran-idUSTRE7B10AV20111202.

E. OUTCOME AND CONSEQUENCES OF STUXNET

Reuters news service reported, "in November 2010, Iranian President Mahmoud Ahmadinejad said that malicious software had created problems in

[257] Michael Kelley, "The Stuxnet Attack on Iran's Nuclear Plant Was 'Far More Dangerous' Than Previously Thought," *Business Insider*, November 20, 2013, http://www.businessinsider.com/stuxnet-was-far-more-dangerous-than-previous-thought-2013-11.

some of Iran's uranium enrichment centrifuges" at Natanz.[258] A network of surveillance cameras, installed by UN weapons inspectors, were already in place at Natanz and provided unfiltered first hand access to the effects of Stuxnet.[259]

Cameras monitoring plant activity captured unexpected images of workers removing suspicious crates full of broken centrifuge equipment.[260] During a six-month period that began in late 2009, UN officials watched Natanz workers dismantle more than 10% of the plants 9,000 uranium enrichment centrifuges.[261] IAEA records from that time show Iran struggling to cope with major equipment failures.[262]

Those same IEAE records also show a concerted and successful effort to limit the damage and replace broken equipment.[263] Although Stuxnet initiated serious malfunctions in the Natanz centrifuges, Iran declared in late 2010 that it had eliminated the malware from its systems.[264] U.S. and European officials, who insisted on anonymity, reported that their experts agreed with the Iranians that they had successfully neutralized Stuxnet and had rooted it from their computers.[265] The Institute for Science and International Security also analyzed the effects of the Stuxnet attack and determined it had slowed the development and progress of the uranium enrichment campaign at Natanz but had not completely disabled it.[266]

---

[258] Hosenball, "Experts Say Iran Has Neutralized Stuxnet Virus."

[259] Warrick, "Iran's Natanz Nuclear Facility Recovered Quickly from Stuxnet Cyberattack."

[260] Ibid.

[261] Ibid.

[262] Ibid.

[263] Ibid.

[264] Hosenball, "Experts Say Iran Has Neutralized Stuxnet Virus."

[265] Ibid.

[266] Warrick, "Iran's Natanz Nuclear Facility Recovered Quickly from Stuxnet Cyberattack."

F. THE FUTURE OF STUXNET

The Stuxnet worm is the first publicly recognized example of a cyber-weapon being used to attack industrial machinery.[267] It provided a blueprint for how to conduct a specifically targeted and innovative cyber-warfare attack on the computer systems of a CI target.[268] More specifically, it shows potential cyber adversaries how to inject malicious code into real time ICS controllers, how to override legitimate control code that remains running, and how to report fake sensor data back to system operators and controllers.[269] This attack is a treasure trove of knowledge and lessons, left behind by the attackers, which may be copied and customized into malware tools to make it available to all.[270]

Opinions have been conflicting as to how Stuxnet spread from its intended target at Natanz. Author David Sanger wrote that an error in the Stuxnet code allowed it to infect an engineer's computer as he worked at Natanz. When he left the plant and connected his computer to the Internet, the Stuxnet worm spread and began replicating itself in other locations around the world.[271] The Symantec Stuxnet dossier attributes the spread of Stuxnet to its programmed replication methods and considers the infected machines outside of Iran to be collateral damage and a necessary consequence of the creators being certain the malware would reach its intended target.[272] The Langer Group theorizes that the attackers may have recognized that blowing their cover could come with benefits and uncovering Stuxnet was the intended end of the operation, as it would show the world what cyber weapons can do in the hands of a competent cyber armed superpower.[273] Regardless of the root cause of the spread of Stuxnet, the result

---

[267] Finkle, "Researchers Say Stuxnet Was Deployed against Iran in 2007."

[268] Karnouskos, "Stuxnet Worm Impact on Industrial Cyber-Physical System Security."

[269] Langer, "To Kill a Centrifuge," 19.

[270] Ibid., 20.

[271] Sanger, "Obama Order Sped Up Wave of Cyberattacks Against Iran."

[272] Falliere, Murchu and Chen, "W32.Stuxnet Dossier," 3.

[273] Langer, "To Kill a Centrifuge," 16.

is that this code is now publicly available to those who are seeking it on the Internet. It could be modified or tailored to stage attacks on the ICS of other CIs throughout the world.[274]

Retired U.S. General Mike Hayden told CBS News, "We have entered into a new phase of conflict in which we use a cyber-weapon to create physical destruction, and in this case, physical destruction to someone else's critical infrastructure."[275] Professor Paul Dorey, of the University of London, notes that it is likely that any form of modern warfare, moving forward, will include attacks on private sector CI to affect that nation's ability to defend itself.[276] This highlights the critical importance of partnerships between privately controlled CIs and government agencies with cyber-defense responsibility.

The Stuxnet worm is the first publicly known use of a cyber-weapon to destroy the CI of another country, accomplishing with computer programming, what only used to be possible through bombing or traditional sabotage.[277] Some researchers, such as Ralph Langer of Germany, believe Stuxnet has opened a "Pandora's Box" for cyber threats that will only increase with time. He makes the point that the next generation of malware, inspired by Stuxnet, will be even more dangerous and difficult to neutralize.[278]

In June 2012, U.S. House Intelligence Committee Chairmen Mike Rogers told CBS News, "We will suffer a catastrophic cyber attack. The clock is ticking."[279] Many of the privately owned CIs in this nation have been slow to invest in updated security measures for their ICS, with some running 30-year-old systems.[280] Cyber security legislative bills have stalled due to fears that

---

[274] Karnouskos, "Stuxnet Worm Impact on Industrial Cyber-Physical System Security."

[275] Kroft, "Stuxnet: Computer Worm Opens New Era of Warfare."

[276] "Cyber Terror Targets Utilities," May 31, 2012, http://www.news24.com/SciTech/News/Cyber-terror-targets-utilities-20120531. News 24.

[277] Sanger, "Obama Order Sped Up Wave of Cyberattacks Against Iran."

[278] Nakashima, "Stuxnet Malware Is Blueprint for Computer Attacks on U.S."

[279] Kroft, "Stuxnet: Computer Worm Opens New Era of Warfare."

[280] Kushner, "The Real Story of Stuxnet."

mandated security updates would be too costly for businesses.[281] The cyber threats to U.S. CI systems are real and this vulnerability is shared between private companies and the government.

[281] Kushner, “The Real Story of Stuxnet.”

THIS PAGE INTENTIONALLY LEFT BLANK

V. STUXNET IMPLICATIONS AND LESSONS

The Stuxnet attack on Natanz was a groundbreaking event with serious implications related to cyber security for CIs, the vulnerability of ICS to manipulation and cyber warfare. The Stuxnet attack was a first of a kind historical event and should be examined for potential lessons learned moving forward. The world's first cyber attack, targeting the CI of a nation, raises a number of yet unanswered questions. With U.S. CI security responsibility split between the government and private sectors, what are the implications? Are the implications for the government and private sectors the same or are they different? What are the implications for our educational system? Does the United States have the experts needed to defend U.S. CI against cyber attacks? Finally, what are the ethical implications involved in both offensive and defensive cyber operations? These topics should be explored, as cyberspace now opens as the fifth domain of warfare, and the first ever-manmade military domain.[282]

A. STUXNET'S EXPLOITATION OF VULNERABILITIES

Stuxnet is a highly refined and complex cyber weapon, designed for stealth that could have avoided detection and done its damage in many CI environments around the world. Therefore, lessons should be extracted and absorbed for U.S. CI cybersecurity. What made a closed system, high security CI facility vulnerable to a cyber attack, absent Internet connectivity? How did the attack manage to spread through the non-networked systems that controlled the Natanz ICS? How was Stuxnet able to work undetected, under the purview of highly trained engineers, and destroy 10% of the facility's centrifuges? These questions may be answered by examining three critical points of failure. The critical points include system access, system security, and policy. These three crucial points all contributed to the failures that allowed Stuxnet to infiltrate, thrive within, and destroy centrifuges at Natanz.

[282] Glenny and Kavanaugh, "800 Titles but No Policy—Thoughts on Cyber Warfare," 288.

Even with all its technological sophistication, the Stuxnet attack on Natanz would not have been possible without the injection of human vulnerability.[283] The first point of failure at Natanz leading to the Stuxnet infection was the insider threat of system access at the facility. Stuxnet was engineered to be hand carried into the Natanz plant to infect the computer network. The Natanz computers were a closed system, absent Internet connectivity, which required Stuxnet to be physically introduced by a device, such as a corrupted removable drive.[284] Symantec experts believe, "this may have occurred by infecting a willing or unknowing third party, such as a contractor who perhaps had access to the facility, or an insider."[285]

Attacks originating from an internal source or insider at a facility have the potential to do the most damage because insiders have direct access to sensitive systems and data. Employees, contractors, and management are all potential inside threats. Insiders also possess the means and knowledge necessary to access information and manipulate systems without raising suspicion.[286] Insider threats are not always intentional. In fact, a 2015 SANS Institute survey of 772 IT security professionals from across the industry spectrum revealed that 69% believed that negligent employees and contractors posed the top cyber security threat to their organizations.[287] This survey provides unique insight into where professionals in the field believe their biggest threats to network security lie.

Insider threats may be divided into two broad categories. The first category involves malicious individuals, with access to a facility, who deliberately create harm. The second category encompasses negligent or accidental insider

---

[283] Jim E. Crouch and Larry K. McKee Jr., "Cybersecurity: What Have We Learned?," National Security Cyberspace Institute, October 9, 2011, 1, http://www.nsci-va.org/WhitePapers/2011-10-09-Cyber%20Lessons%20Learned-Crouch-McKee.pdf.

[284] Hosenball, "Experts Say Iran Has Neutralized Stuxnet Virus."

[285] Falliere, Murchu, and Chen, "W32.Stuxnet Dossier," 3.

[286] Roy Urrico, "Negating Cybersecurity Threats from Within," *Credit Union Times,* June 3, 2015, http://search.proquest.com/docview/1685156530?accountid=12702.

[287] Eric Cole, "Insider Threats and the Need for Fast and Directed Response," SANS Institute, April 2015, 6, https://www.sans.org/reading-room.

threats. It involves individuals with access to facilities or networks who do not follow established security practices and breed vulnerability through the improper handling of data, systems, and networks.[288] The individuals in this second category typically do their damage without the actual intent to do harm. Their actions may be simply characterized as unaware, unconcerned, lazy, or careless.

Netdiligence is a cyber risk assessment and data breach services company that conducts an annual cyber insurance claims study each year. It started collecting data on insider involvement in cyber damage claims to insurance companies two years ago, and its survey findings have been comparable for the past two years. The 2015 report notes approximately one third of all cyber insurance claims paid out were determinable to insider vulnerabilities. Of those 2015 insider damage claims, two thirds were unintentional in nature.[289]

The Sans and Netdiligence surveys highlight a notable point. Insider threats are receiving growing notoriety among IT industry professionals as a major vulnerability. Insiders are also doing their part to justify this anxiety, with much of their damage being done unintentionally. The fact remains that negligent insiders spawn potential network access portals for malicious outsiders and incubate potential vulnerability for CI in the United States. No one may ever know specifically who infected Natanz, but it is clear that insider access played a paramount role in the attack. The same vulnerabilities likely exist within many U.S. CIs.

The second point of failure at Natanz was the spread of Stuxnet through an air-gapped network to the PLCs, which controlled the precise spinning speed needed for proper centrifuge operations. Once Stuxnet infiltrated the Natanz network, through an infected removable drive host, it still had to move through the air-gapped computers to the PLCs, which controlled the precise spin speeds

[288] Urrico, “Negating Cybersecurity Threats from Within.”

[289] “2015 Cyber Claims Study,” September 2015, 25, http://netdiligence.com/articles.php.

of the plant's centrifuges. In this instance as well, Stuxnet was cleverly engineered to take advantage of a systemic weakness.

Isolated and air gapped systems, such as the one at Natanz, have limited options when it comes to moving data between physically separated network computer systems.[290] Stuxnet was programmed to copy itself onto inserted removable drives, each time one was used, as one of its primary propagation methods. Thus, each time an infected removable drive was used to move data or instructions from one computer to another, the Stuxnet worm was also implanted. This move exploited the closed system environment of Natanz in which operators exchanged data with other computers by using removable drives, which thus spread Stuxnet continuously throughout the facility from computer to computer.[291] Stuxnet also had the ability to replicate itself and autonomously spread through networked systems once it infected a host computer with network access.[292]

These first two points of failure, system access and system security, fall into line with the third point of failure, which is policy. Although the Iranian government will not publicly share its Natanz policy portfolio, a deficiency in either establishing or following appropriate security protocols led to the system access and system security breakdowns noted as the first two points of failure. Effective technology security policy should focus inward on vulnerabilities rather than outward toward threats, due to the ever-evolving nature of cyber threats.[293]

Insiders were highlighted earlier as an important threat vector according to cybersecurity experts; thus, human factors related to protecting CI ICS systems should not be neglected. Stuxnet is a glaring example of vulnerability posed by insider threats since an insider with a removable drive introduced it. Policy and

[290] Doug Niblick, "Protecting Critical Infrastructure against the Next Stuxnet," Davenport University, March 20, 2013, 19, http://www.davenport.edu/system/files/Protecting_Critical_Infrastructure_Against_the_Next_Stuxnet.pdf.

[291] Falliere, Murchu, and Chen, "W32.Stuxnet Dossier," 29.

[292] Ibid., 25.

[293] Crouch and McKee Jr., "Cybersecurity: What Have We Learned?," 2.

procedure related to insider access should be effectively written, communicated, and enforced to limit system and sensitive data access to the smallest number of authorized users possible.[294] The policy should extend beyond employees to management, visitors, contractors, and even business partners. The objective is to restrict access as tightly as possible, while still allowing for efficient business operations, to narrow the insider threat vector as much as possible.

Stuxnet's propagation through the Natanz computer systems could also have been affected from a technology security policy standpoint. Removable drive infections are known to be common.[295] Policy restrictions on the use of portable media and drives, along with the encryption of sensitive system data, could have greatly reduced the vulnerability at Natanz had such restrictions been followed.[296] Data could still be securely moved through air-gapped CI systems like Natanz on removable storage drives with specific removable drive security software that is backed up by policies specifying which devices can be used and by whom.

Michael Davis, of Information Week Analytics, wrote an article entitled, "Stuxnet Reality Check: Are You Prepared for a Similar Attack?"[297] He asserts that "removable storage device security software" is the most effective countermeasure to USB infections.[298] Davis writes further, "removable storage device security software prevents unknown or unauthorized USB drives, CDs/DVDs, external drives, digital music players," and other devices that could carry infections, from being accepted by and uploading data to facility computers.[299] Davis maintains, "These tools should be utilized and reinforced

---

[294] Niblick, "Protecting Critical Infrastructure against the Next Stuxnet," 21.

[295] Crouch and McKee Jr., "Cybersecurity: What Have We Learned?," 7.

[296] Niblick, "Protecting Critical Infrastructure against the Next Stuxnet," 18.

[297] Michael A. Davis, "Stuxnet Reality Check: Are You Prepared for a Similar Attack?" Information Week Analytics in conjunction with Security Dark Reading, May 2011, 14, http://i.techweb.com/darkreading/advancedthreat/S2840511_DR_stuxnet.pdf.

[298] Ibid.

[299] Davis, "Stuxnet Reality Check: Are You Prepared for a Similar Attack?" 14.

with policies that specify which, if any, removable storage devices can be used on a particular computer and by whom."[300] The facility may then close the system's communication loop by providing authorized users with the acceptable authorized drives for data transfer that the software will validate before connecting.[301] The reinforcement of strong policy defenses with technology further strengthens CI computer network defense.

B. IMPLICATIONS FOR A CI CYBER ATTACK ON THE UNITED STATES

Increasing concern has been raised among government officials and private sector experts about the cyber security of the ICS that govern U.S. CIs. U.S. government experts were interviewed for a CBS News 60 Minutes episode entitled "Stuxnet," which aired on March 4, 2012. The interviews resulted in some candid quotes revealing how consequential of a threat a cyber attack, similar to Stuxnet, could be to the United States. Former Defense Secretary Leon Panetta stated, "There's a strong likelihood that the next Pearl Harbor that we confront could very well be a Cyberattack." Former FBI Director Robert Mueller was quoted as saying, "I do believe that the cyberthreats will equal or surpass the threat from counterterrorism in the foreseeable future." Former House Intelligence Committee Chairman Mike Rogers said, "We will suffer a catastrophic cyberattack. The clock is ticking."

Technological advances have led to ICS components making increasingly critical automated decisions, in industrial processes, which used to be the responsibility of human operators. These advances have spawned enhanced CI vulnerability to ICS cyber attacks and makes those attacks potentially even more consequential.[302] According to Nasser Abouzakhar, of the University of Hertfordshire, the manipulation of intricate processes in ICS can cause "threshold

[300] Ibid.

[301] Ibid.

[302] Boaru and Badita, "Critical Infrastructure Protection Challenges and Efforts to Secure Control Systems," 154.

levels to build beyond safe operating parameters."[303] He continues that this manipulation, may, in turn, result in disasters, the loss of lives or a long-term loss of vital services.[304] A foreign intelligence service or high functioning terrorist group, with sufficient resources, could undertake a nearly anonymous cyber attack on the U.S. electric power grid without ever entering the country.[305]

The potential impacts of a CI cyber attack targeting ICS could be a combination of physical, economic, and social effects. Physical impacts are the direct result of an ICS failure and include personal injury, loss of lives, and property and environmental damage.[306] Economic impacts are a second order effect resulting from the physical impact. Unavailability of damaged CI may have long standing negative effects to the local, regional, and national economy.[307] Social impacts are another second order effect that includes the loss of confidence by the public in the company or government entity operating a CI impacted by a cyber attack.[308]

Numerous potential consequential events may result from a cyber attack to a CI or an ICS component of a CI. A number of these consequential events are common to many of the sectors, while others are more individualized. Some of the potential consequences include: injury or death of employees; injury or death of citizens; damage to equipment and property; loss of production capability; release, diversion, or theft of hazardous materials; environmental damage; long or short term loss of critical services; product contamination; criminal or civil liability; loss of confidential information; loss of customer

[303] Abouzakhar, "Critical Infrastructure Cybersecurity: A Review of Recent Threats and Violations," 3.

[304] Ibid.

[305] Boaru and Badita, "Critical Infrastructure Protection Challenges and Efforts to Secure Control Systems," 154.

[306] Stouffer et al., *Guide to Industrial Control Systems Security*, 4–3.

[307] Ibid.

[308] Ibid.

confidence; and impacts on national security.[309] Table 1 highlights potential cyber attack impacts for the 16 CI sectors.

[309] Stouffer et al., *Guide to Industrial Control Systems Security*, 4–3.

Table 1. CI Cyber Attack Consequences

Chemical Sector	• Injury or death of employees or the public • Release, diversion or theft of hazardous materials • Environmental damage
Commercial Facilities Sector	• Loss of lives • Civil liability • Loss of customer confidence
Communications Sector	• Loss of critical service availability • Damage to equipment and property • Economic damage
Critical Manufacturing Sector	• Impact on national security • Loss of production capacity • Economic damage
Dams Sector	• Loss of lives • Environmental damage • Property damage
Defense Industrial Base Sector	• Impact on national security • Loss of production capacity • Economic damage
Emergency Services Sector	• Long or short term loss of critical services • Lives and property left at risk • Loss of public confidence in government
Energy Sector	• Loss of production capacity • Economic damage • Lives and property left at risk
Financial Services Sector	• Economic damage • Loss of customer confidence in banking • Loss of business production capability
Food and Agriculture Sector	• Product contamination and risk to human lives • Loss of production capability • Economic damage
Government Facilities Sector	• Long or short term loss of critical services • Damage to equipment and property • Loss of public confidence in government
Healthcare and Public Health Sector	• Long or short term loss of critical services • Injury or death of citizens • Civil liability
Information Technology Sector	• Long or short term loss of critical services • Loss of confidential information • Impact on national security
Nuclear Reactors, Materials and Waste Sector	• Release, diversion or theft of hazardous materials • Environmental damage • Impact on national security
Transportation Systems Sector	• Loss of transportation services • Injury or death of citizens • Economic damage
Water and Wasewater Systems Sector	• Drinking water contamination • Injury or death of citizens • Environmental damage

According to NIST, “U.S. critical infrastructure is often referred to as a ‘system of systems’ because of the interdependencies that exist between its various industrial sectors as well as interconnections between business partners.”[310] This interconnection and mutual dependency results in a phenomenon where an issue at one CI can directly disrupt other CIs through “cascading and escalating failures.”[311] Electric power failures are a common example of cascading disruptions to interdependent CIs.[312] Power outages affect every other CI sector because they all rely on electrical power to operate.

NIST points out, “A cascading failure can be initiated by a disruption of the microwave communications network used for an electric power transmission SCADA system.”[313] NIST adds, “the lack of monitoring and control capabilities could cause a large generating unit to be taken offline, an event that would lead to loss of power at a transmission substation.”[314] The transmission substation failure could create, “a major imbalance, which triggers a cascading failure across the power grid.”[315] That grid failure could result in, “large scale blackouts that could potentially affect oil and natural gas production, refinery operations, water treatment systems, wastewater collection systems, and pipeline transport systems that rely on the grid for electric power.”[316]

Other potential consequences of an electric grid failure include failures of telephone communications networks, public safety radio systems, chemical plants, and hazardous materials facilities, which could all endanger public health,

---

[310] Stouffer et al., *Guide to Industrial Control Systems Security*, 2–2.

[311] Ibid., 2–3.

[312] Steven M. Rinaldi, James P. Peerenboom, and Terrence K. Kelly, “Identifying, Understanding, and Analyzing Critical Infrastructure Interdependencies,” *IEEE Control Systems Magazine*. December 2001, 11, http://user.it.uu.se/~bc/Art.pdf.

[313] Stouffer et al., *Guide to Industrial Control Systems Security*, 2–3.

[314] Ibid.

[315] Ibid.

[316] Ibid.

public safety, and the environment.[317] The possibilities for both cascading CI failures between interdependent sectors, and their resulting potential consequences, are nearly endless. Cyber security for vulnerable CI ICS must be a top priority to ensure the orderly function of every segment of modern society.

C. IMPLICATIONS FOR THE GOVERNMENT AND PRIVATE SECTORS

Stuxnet's implications for the U.S. government and private sectors are intertwined, much like the infrastructure itself, and highlight the necessity of coordination between the sectors as it pertains to protecting U.S. CI ICS from cyber threats. As noted by the DHS:

> Cyberspace is particularly difficult to secure due to a number of factors: the ability of malicious actors to operate from anywhere in the world, the linkages between cyberspace and physical systems, and the difficulty of reducing vulnerabilities and consequences in complex cyber networks. Of growing concern is the cyber threat to critical infrastructure, which is increasingly subject to sophisticated cyber intrusions that pose new risks.[318]

The DHS contends that as computer technology innovates and continues to integrate with operational CI processes, an increased vulnerability occurs to elevated-consequence cyber incidents that could create damage, threaten lives, or interfere with the crucial services on which Americans count.[319] With this risk and consequence in mind, the DHS considers "strengthening the security and resilience of cyberspace" a crucial "homeland security" mission.[320] Societal reliance on technological innovation, and the inherent threats from within the cyber realm, will only increase in the years to come.

The U.S. government response to the emerging class of cyber threats has been bifurcated between the military and civilian sectors. The U.S. government

---

317 Ibid.

318 "Cybersecurity Overview," U.S. Department of Homeland Security, last modified September 22, 2015, http://www.dhs.gov/cybersecurity-overview.

319 Ibid.

320 Ibid.

identified cyberspace as the fifth domain of warfare.[321] In June 2009, the Secretary of Defense ordered the Commander of the U.S. Strategic Command to institute a new cyber focused sub-command. In October 2010, the United States Cyber Command (USCYBERCOM) emerged as fully operational from its headquarters at Fort Meade, MD. Its mission is defined as:

> USCYBERCOM plans, coordinates, integrates, synchronizes and conducts activities to: direct the operations and defense of specified Department of Defense information networks and; prepare to, and when directed, conduct full spectrum military cyberspace operations in order to enable actions in all domains, ensure US/Allied freedom of action in cyberspace and deny the same to our adversaries.[322]

Although its responsibilities are clearly militarily focused, it is important to note that cyber attacks on CI may be considered acts of war that could draw USCYBERCOM into the defense of CIs within the United States.

On the domestic front, the DHS bears responsibility for the difficult task of CI cyber defense and attack mitigation. The DHS utilizes what it describes as a "risk informed, all hazards approach to safeguarding CI in cyberspace."[323] The DHS also takes the lead role in coordinating with, "sector specific agencies, other federal agencies and private sector partners to share information of analysis on cyber threats and vulnerabilities to promote and to understand more fully of the interdependency of infrastructure systems nationwide."[324] The DHS reports its collective approach is to "prevent, protect against, mitigate, respond to, investigate, and recover from cyber incidents prioritizes understanding and meeting the needs of our partners, and is consistent with the growing recognition

---

[321] Angelyn Flowers and Sherali Zeadally, "U.S. Policy on Active Cyber Defense," *Journal of Homeland Security and Emergency Management* 11, no. 2 (2014): 299, doi:http://dx.doi.org/10.1515/jhsem-2014-0021.

[322] "U.S. Cyber Command," March 2015, https://www.stratcom.mil/factsheets/2/Cyber_Command/.

[323] "Protecting Critical Infrastructure," September 23, 2015, http://www.dhs.gov/topic/protecting-critical-infrastructure.

[324] Ibid.

among corporate leaders that cyber and physical security are interdependent and must be core aspects of their risk management strategies."[325]

The private sector's ownership of approximately 85% of U.S. CI[326] makes it potentially the vulnerable soft underbelly of this country's CI cyber protection posture. Furthermore, some companies or industries may be more effective than government entities in implementing protection strategies. However, the fragmented nature of private sectors makes uniform measures and the implementation of best practices very difficult to achieve. Even though some industries have professional or technical associations for their respective fields, each organization is ultimately individually driven.

Segments of the U.S. private sector philosophically object to government mandated cybersecurity measures. Some consider such measures to be an unnecessary layer of extra government regulation.[327] Others argue that mandating cybersecurity measures will actually hamper cybersecurity innovation within the private sector. The U.S. Chamber of Commerce has actually taken an official position against any legislation establishing private sector cybersecurity standards.[328]

When talking about private industry motivation, profit is certainly a driving factor in business. Compelling private sector companies to improve cybersecurity carries a substantial price tag that could affect short-term profits. Some organizations believe that since the United States has not suffered a prominent cyber disruption of control systems, spending the time and money to prematurely

---

325 "Protecting Critical Infrastructure."

326 U.S. Government Accountability Office, *Critical Infrastructure Protection—Progress Coordinating Government and Private Sector Efforts Varies by Sectors' Characteristics*, 1.

327 Amitai Etzioni, "The Private Sector: A Reluctant Partner in Cybersecurity," The George Washington University, December 19, 2014, https://icps.gwu.edu/private-sector-reluctant-partner-cybersecurity.

328 Ibid.

update security for ICS is not economically justifiable when their current systems were designed to have 20+ year lifespans.[329]

Although the DHS has a few voluntary programs for private sector CI, their key focal point to the national strategy for securing U.S. government and private sector ICS is the Industrial Control Systems Cyber Emergency Response Team (ICS-CERT). ICS-CERT responds to investigate ICS incidents; conducts vulnerability analyses; provides onsite incident response services; provides actionable intelligence for situational awareness; coordinates the discrete disclosure of vulnerabilities and mitigations; and provides information products and alerts regarding vulnerabilities and threats.[330] ICS-CERT also coordinates information sharing with federal, state, and local agencies, the intelligence community, and private sector constituents to provide a direct pipeline for coordination among all stakeholders.[331]

D. EDUCATIONAL AND WORKFORCE IMPLICATIONS

A potentially overlooked but vitally important implication of the Stuxnet attack focuses on the education and skill sets of the people employed to protect U.S. CIs from cyber attacks in both the private and government sectors. Rapid technical innovations and advancements in computer technology within U.S. CIs require the services of an increasingly technologically astute workforce. Uncertainty surrounds U.S. capability to educate and train a sufficiently educated and sized workforce in cyber defense. This uncertainty is a concern within both the government and private sectors, which actually compete with each other for talent, as job requirements grow increasingly more technical and complex. The U.S. capacity to maintain it's standing as a technology innovator is key to the nation's ability to protect U.S. CIs and their computerized ICS from future attacks.

---

[329] Boaru and Badita, "Critical Infrastructure Protection Challenges and Efforts to Secure Control Systems," 157.

[330] "About the Industrial Control System Cyber Emergency Response Team," accessed October 24, 2015, https://ics-cert.us-cert.gov/About-Industrial-Control-Systems-Cyber-Emergency-Response-Team.

[331] Ibid.

The Institute for National Strategic Studies researched this key vulnerability and found, "widespread agreement in the public and private sectors that U.S. educational institutions are unable to meet the growing demand for cyber workforce professionals."[332] A March 2015 study of Bureau of Labor Statistics data revealed that more than 209,000 U.S. cyber security jobs were unfilled.[333] Postings for cyber security jobs are up 74% over the past five years and demand for these types of jobs is expected to grow by 53% through the year 2018.[334] The United States currently has a gap to fill in being able to educate and train enough talent for the workforce, fast enough to keep up with the current pace of hiring. The resultant outcome of this gap is the frequent raiding of talent from government agencies or competitors by the cyber security and private industries.[335]

The cornerstone educational fields within the cyber security realm have long been considered science, technology, engineering and mathematics (STEM).[336] These disciplines will always be pertinent to the field but a need exists to cast a wider net to capture more multidisciplinary focused students while increasing the traditional talent pool. The foundation for effective secondary education takes place at the K-12 level. Ensuring the strength of the primary level STEM curriculum is a key element to ensuring the future security of U.S. CIs. School districts must also find ways overcome budget-constrained environments

[332] David J. Kay, Terry J. Pudas, and Brett Young, "Preparing the Pipeline: The U.S. Cyber Workforce for the Future," *Defense Horizons,* no. 72 (August 2012): 1–2, http://search.proquest.com/docview/1038377323?accountid=12702.

[333] Ariha Setalvad, "Demand to Fill Cybersecurity Jobs Booming," Peninsula Press of Stanford, March 31, 2015, http://peninsulapress.com/2015/03/31/cybersecurity-jobs-growth/.

[334] Ibid.

[335] Christophe Veltsos, "Addressing the Information Security Skills Gap in Partnership with Academia," Security Intelligence, October 9, 2015, https://securityintelligence.com/addressing-the-information-security-skills-gap-in-partnership-with-academia/.

[336] Kay, Pudas, and Young, "Preparing the Pipeline: The U.S. Cyber Workforce for the Future," 4.

and shortages of qualified teachers to find ways to expose students to classes in programming and computer science.[337]

E. ETHICAL IMPLICATIONS

The Stuxnet attack on Iran's uranium enrichment program at Natanz has ushered in a new era of non-traditional conflict and raises a number of new ethical issues. Stuxnet raised the bar from wreaking cyber havoc to wreaking physical destruction, and as such, has released the proverbial cyber genie from the bottle and that genie will not be returning to confinement.[338] Dilemmas posed, such as active vs. passive cyber defense, determining attribution of cyber attacks, discrimination in responses, proportionality in responses, and the consequences of escalation, affect the military, government, and private sector sectors alike.

The GAO reports that during the 9-year period from 2006–2014, the number of CERT reported cybersecurity incidents directed toward systems supporting CI and federal operations rose by a staggering 1,120 percent, from 5,503 in 2006 to 67,168 in 2014.[339] It is not surprising that in light of this trend, President Obama authorized the U.S. government, in PPD 20, to employ defensive cyber effect operations on behalf of private sector organizations to protect CIs against cyber attacks.[340] This possibility, does however, create interesting shared ethical dilemmas for the military, government, and private sectors.

Cyber defense strategies can range anywhere from and in between merely stopping or preventing attacks to punishing cyber adversaries to deter

---

[337] Ibid.

[338] Ryan Jenkins, "Is Stuxnet Physical? Does it Matter?," in *Military Ethics and Emerging Technologies,* ed. Timothy J. Demy, George R. Lucas Jr., and Bradley J. Strawser (London and New York: Routledge, 2014), 263–264.

[339] Gene L. Dodaro, *Report to Congressional Committees: High-Risk Series, an Update* (GAO-15-290) (Washington, DC: U.S. Government Accountability Office, 2015), 242, http://www.gao.gov/assets/670/668415.pdf.

[340] Flowers and Zeadally, "U.S. Policy on Active Cyber Defense," 296.

future attacks. Some have even labeled the U.S. move of indicting five Chinese Army officers, for hacking and commercial espionage in 2014, a unique public "shaming" tactic to try to leverage cultural pressures.[341] Cyber defenses to attacks, such as Stuxnet, typically are either "passive" countermeasures to repel attacks or "active" countermeasures taking direct action against a threat.[342]

Passive cyber defenses are designed to prohibit entry into a system, or if entry is made, to neutralize the threat and prevent damage, corruption of data systems, or the theft of information. These internal measures carry few ethical implications since they are focused inward but are commonly viewed as inadequate in defeating today's advanced persistent threats from external sources.[343] The inadequacy of passive cyber defense strategies alone sheds light on the potential need to field an ability to defend key cyber assets through the use of active cyber defenses.

Active cyber defenses fall into the three general categories of detection and forensics, deception, and attack termination.[344] These methods have three primary advantages. They assist in establishing the identity of the attacker; they may deter future attacks through retaliatory fear, and they can actually knock imminent cyber attacks off line.[345] However, potential unintended consequences can occur, which may result from active cyber defense measures. The ethical waters get a little murky due to an attacker's ability to disguise web attack vectors. A nation mistakenly employing active cyber defense countermeasures against an innocent party embroils itself in both ethical and legal issues. Attributing attacks to responsible parties, discriminating targeted responses to

---

[341] Jeremy Yonah, "U.S. Tries Policy of 'Shame' to Stem Chinese Cyber-Hacking," *Jerusalem Post,* August 17, 2014, http://search.proquest.com/docview/1555615443?accountid=12702.

[342] Dorothy E. Denning, "Framework and Principles for Active Cyber Defense" (essay, Naval Postgraduate School, 2013), 3, http://faculty.nps.edu/dedennin/publications/Framework%20and%20Principles%20for%20Active%20Cyber%20Defense%20-%2011Dec2013.pdf.

[343] Flowers and Zeadally, "U.S. Policy on Active Cyber Defense," 292.

[344] Ibid., 293.

[345] Ibid.

avoid collateral damage, and keeping responses proportional are all challenging but necessary components of ethical active cyber defense.

Assuming that an attack, such as Stuxnet, justifies an active cyber response, attributing the attack to a responsible party can be very difficult. Sometimes, a victimized entity may have no idea who the attacker is or may only be able to narrow the possibilities to "possible" or "probable."[346] Even worse, computer technology may now be used to mask certainty about the attacker's location, equipment, identity, affiliation, or even implicate innocent parties.[347] Active cyber defense measures would only be ethically justifiable with certainty as to the aggressor's identity.

Discrimination is another key ethical issue related to cyber weapons. Although Stuxnet ultimately infected both military and civilian networks, it had safety measures programmed within the code to ensure that it only took action upon military targets within Natanz.[348] However, in nations such as the United States, the government and military rely primarily on privately owned and operated communications networks. Active cyber countermeasures targeting government command and control would necessitate targeting civilian CI in many cases, which would create civilian collateral damage in the form of disrupted personal and commercial communications.[349]

Proportionality is another ethical dilemma brought to the forefront by the active response to cyber attacks. The use of force in international law is generally limited to that which is needed to stop an attack. As such, cyber defense response options are in many ways ethically bound by the actions of the

---

[346] John Arquilla, "Twenty Years of Cyberwar," in *Military Ethics and Emerging Technologies,* ed. Timothy J. Demy, George R. Lucas Jr., and Bradley J. Strawser (London and New York: Routledge, 2014), 276.

[347] Edward T. Barrett, "Warfare in a New Domain: Ethics of Military Cyber-Operations," in *Military Ethics and Emerging Technologies,* ed. Timothy J. Demy, George R. Lucas Jr., and Bradley J. Strawser (London and New York: Routledge, 2014), 203.

[348] Jenkins, "Is Stuxnet Physical? Does it Matter?," 269.

[349] Arquilla, "Twenty Years of Cyberwar," 279–280.

perpetrator.[350] In response, however, the entity deploying an active cyber defense must be aware of the effects of that response, even to third parties.[351] An adversary habitually stealing state or corporate secrets would justify only a proportional response that would not affect third parties.[352] For example, a DDoS on the servers of an entity deemed to be committing ongoing thefts of secrets could cause disproportionate harm if that response took critical life support equipment off line at a medical facility.[353]

It is debatable whether cyber attacks violate another state's sovereignty or not. Since cyber attacks may not necessitate a physical presence in a state, and transmitted software is not necessarily physical, it could be argued that a nation's territorial integrity was not violated.[354] Therefore, a valid self-defense claim might not apply.[355] Despite these arguments and dilemmas, what is most relevant are the consequences, such as whether cyber actions caused physical damage or tangible harm.[356] Differentiation between active cyber defenses, and offensive cyber operations, such as Stuxnet, can be subjective and open to interpretation.[357] Thus, the real potential for escalating cyclic cyber responses is created. Perhaps, an even more threatening result to the ethical dilemmas posed by cyber attacks is the further escalatory response possibility of crossing the threshold to physical retaliation in the form of military action.[358] These are all ethical dilemma's arising from attacks, such as Stuxnet, that will be sorted out and debated for years to come as the cyber threat landscape continues to grow.

---

[350] Flowers and Zeadally, "U.S. Policy on Active Cyber Defense," 299.

[351] Denning, "Framework and Principles for Active Cyber Defense," 7.

[352] Barrett, "Warfare in a New Domain: Ethics of Military Cyber-Operations," 201.

[353] Denning, "Framework and Principles for Active Cyber Defense," 8.

[354] Jenkins, "Is Stuxnet Physical? Does it Matter?," 267.

[355] Flowers and Zeadally, "U.S. Policy on Active Cyber Defense," 298.

[356] Jenkins, "Is Stuxnet Physical? Does it Matter?," 268.

[357] Flowers and Zeadally, "U.S. Policy on Active Cyber Defense," 305.

[358] Arquilla, "Twenty Years of Cyberwar," 277.

THIS PAGE INTENTIONALLY LEFT BLANK

VI. CONCLUSIONS AND POLICY RECOMMENDATIONS

Policymakers and industry experts have exhibited growing concern over CI cyber security for the past two decades. CIs are the lifeblood of contemporary civilization, and fuel the delivery of the crucial services that underpin the modern way of life. Cyber attacks on CI facilities could result in devastating physical, economic, and social consequences for communities. U.S. policy has been shaped over the past two decades by a growing recognition of cyber threats and the importance of cyber security, but those policies have not always been clearly articulated and streamlined nor consistently communicated.

A. OVERVIEW OF RELEVANT ISSUES

CI systems have evolved to be increasingly networked and computer reliant. The industrial and mechanical processes of many of these systems are now monitored and controlled by computerized ICS. The interjection of autonomous computer technology into these operational processes has opened the door to cyber vulnerability. The 16 U.S. CI sectors have also evolved toward a state of interdependence that creates a heightened risk of cascading failures with far-reaching effects for multiple sectors in simultaneous events. The stakeholders tasked with responsibility for securing the 16 CI sectors in the United States are blended between the public and private sectors, which makes mandated compliance with cyber security best practice a daunting challenge.

Security experts view the Stuxnet attack on Iran as a game changer. It is universally recognized as the first politically motivated cyber attack, targeting the CI of a nation, which created physical destruction. Many have likened it to the opening of a cyber Pandora's Box as a new domain for terrorism, espionage, and military action. Stuxnet does expose educational, ethical, and legal challenges. Nations will need to field technically educated work forces to secure their cyber space and CIs from attacks. Ethical and legal boundaries need to be defined and

legally clarified within and across the international community, as it pertains to cyber offensive and defensive operations.

B. U.S. VULNERABILITY TO CYBER ATTACKS

Despite the securing of cyberspace becoming a growing national policy priority, the United States continues to be the target of a continuous stream of cyber attacks. Many of these attacks are directed at the CIs, which support the normal daily routine of the lives of Americans and the nation as a whole. A crippling malware attack to computer networks of CIs could be economically devastating and could even lead to the loss of lives. Disruptions in service could affect the government's ability to provide basic domestic or international security services, create gaps in essential public sector services for lengthy periods of time, and foster a loss of public confidence in government.[359] An examination of four recent cyber attacks targeting U.S. CI follows.

United Airlines announced on July 29, 2015 that it had sustained a data breach of passenger manifest data in May or early June 2015. This information detailed the movement of millions of Americans, to include some who hold sensitive positions within government and industry. A foreign government is believed to have been responsible for this breach and could exploit this information in a number of ways.[360] A foreign intelligence agency could cross-reference passenger manifest data with the data stolen in the U.S. Office of Personnel Management (OPM) computer system breach. The OPM data identifies people in sensitive government positions who hold security clearances. Tracking the movements of such officials could expose key meeting sites, classified events, or even covert operations or personnel.

On July 25, 2015, the unclassified email network servers of the Joint Chiefs of Staff, of the DOD, were accessed remotely following a "spear phishing" email ruse used to gain access to the system. This intrusion necessitated an 11-

[359] Kerr, Rollins, and Theohary, *The Stuxnet Computer Worm*.

[360] "Cyber Incident Timeline," July 29, 2015, http://www.csistech.org/cyber-incident-timeline/.

day shutdown of the network so it could be rebuilt and reconfigured. The work of nearly 4,000 military and civilian personnel was affected for the duration of the shutdown. Breaches of defense sector networks can directly impact the military's ability to provide for national safety and security. It is suspected that a foreign government is responsible for this intrusion.[361]

On June 4, 2015, OPM announced it had sustained two separate attacks over the past year, which resulted in the theft of very detailed personal information on 25.6 million government employees and security clearance holders. Nearly every federal agency, and numerous CI sectors, was struck as part of this attack. Intelligence agents believe a foreign government attempting to build a database on U.S. government employees sponsored this theft.[362]

The implication for the identities of all U.S. security clearance holders to be known by a foreign government highlights significant vulnerabilities. One major concern would be the data being used by foreign governments to recruit U.S. government employees, who might be vulnerable to enticements or pressure, to spy on their behalf.[363] Another concern would be a foreign intelligence agency using the information to uncover the true identities of Central Intelligence Agency (CIA) covert agents. Even though CIA data was largely shielded from this breach, operatives who formerly worked for other government agencies could be exposed. Additionally, foreign intelligence services could cross-reference U.S. embassy roster data with that from the OPM breach to identify, through a process of elimination, CIA officers stationed at foreign embassies who work under diplomatic cover.[364]

---

361 "Cyber Incident Timeline."

362 Ibid.

363 Ellen Nakashima, "Hacks of OPM Databases Compromised 22.1 Million People, Federal Authorities Say," *Washington Post*, July 9, 2015, https://www.washingtonpost.com/news/federal-eye/wp/2015/07/09/hack-of-security-clearance-system-affected-21-5-million-people-federal-authorities-say/.

364 Ibid.

On April 8, 2015, the United States reported that Russian hackers had gained access to unclassified but sensitive White House computer networks, through State Department networks that have been previously compromised. Adversaries were able to access information that included emails sent and received by President Obama, and real time information about his schedule that was not available to the public. This probing of privileged presidential information has far reaching potential ramifications and could put both national security and people's lives at risk.[365]

The four previously mentioned examples occurred within a short four-month window during 2015. Others could be listed, but these attacks clearly demonstrate a current cyber vulnerability not being adequately addressed through current U.S. policy and practice.

C. CI VULNERABILITY AND EMERGING GLOBAL EMPHASIS ON CYBER WEAPONS PROGRAMS

Thus, what makes exploring solutions to the cyber security CI threat worthy of premium policy prioritization in a world full of threats? Recent research by the Unisys Corporation revealed distressing cyber vulnerability within the world's CIs. Their 2014 survey quizzed "599 security executives at utility, oil, gas, energy and manufacturing companies" and found that 70% reported "at least one cyber security breach" resulting in the loss of proprietary data or the "disruption of operations" within the preceding twelve months.[366] They were also questioned as to their opinions on the probability that their institutions would sustain an ICS cyber attack, and "78% responded that a successful attack is at least somewhat likely within the next 24 months."[367] Finally, "64% of respondents anticipated one

[365] Nakashima, "Hacks of OPM Databases Compromised 22.1 Million People, Federal Authorities Say."

[366] "United States: Unisys Survey Reveals Nearly 70 Percent of Critical Infrastructure Providers Have Been Breached in the Past Year," July 11, 2014, http://search.proquest.com/docview/1544450370?accountid=12702.

[367] Ibid.

or more serious attack(s) within the next year" but "only 28% ranked security as one of the top five strategic priorities for their organizations."[368]

This CI vulnerability is coupled to what many believe is a new cyber arms race. In the past, joining other nations with nuclear weapons capability has always been an expensive and technologically difficult undertaking for aspiring nations. However, developing and fielding a cyber weapons arsenal is much less expensive and easier to accomplish. According to a *Wall Street Journal* compilation of government records and interviews, at least 29 countries have formalized intelligence or military units dedicated to offensive cyber operations.[369] In recognition of the growing cyber threat, the U.S. Cyber Command currently fields nine "national mission teams" and plans to add four more.[370] According to a Pentagon spokesperson, the mission teams will, "Conduct full spectrum cyberspace operations to provide cyber options to senior policy makers in response to attacks against our nation."[371] Cyberspace is an expanding frontier for military and intelligence operations that will continue to evolve as fast as technology does.

D. POLICY RECOMMENDATIONS

The objective of this thesis is to identify the pivotal areas of U.S. policy that could be enhanced to provide the most effective overarching solutions to the current vulnerabilities highlighted within this document, and then provide recommendations for the improvement of these key areas. The three key areas in need of policy enhancement to bolster the national CI and ICS defenses include enhancing national unity of effort, expansion of cyber security

368 "United States: Unisys Survey Reveals Nearly 70 Percent of Critical Infrastructure Providers Have Been Breached in the Past Year."

369 Damian Paletta, Danny Yadron, and Jennifer Valentino-DeVries, "Cyberwar Ignites New Arms Race," *Wall Street Journal*, October 12, 2015, http://www.wsj.com/articles/cyberwar-ignites-a-new-arms-race-1444611128.

370 Ibid.

371 Ibid.

coordination between the private and government sectors, and incentivizing private sector compliance with best practices in cyber security.

1. Enhancing National Unity of Effort

Achieving national unity of effort is a crucial and fundamental objective of national CI cyber security policy due to the diverse stakeholder pool responsible for national CI cyber security, and the far-reaching societal effects of a successful cyber attack on CIs. Securing cyberspace, and the computer networked CIs that interact within it, has become a national policy priority for the U.S. government. However, defining U.S. policy, as it pertains to CI cyber protection, is made difficult due to the overlapping nature of the various documents, which make up the policy. The policy must be distilled from continually evolving documents, such as legislation, commission reports, presidential decision directives, EOs and official federal plans. Changes in presidential administrations have each triggered a cycle of restructuring, realigning, renaming, and refocusing of efforts and objectives.

Although U.S. CI cybersecurity policy has evolved greatly over the past two decades, it is a complex interwoven fabric comprised of a variety of types of national policy documents. The policy has evolved from an initial focus on physical security to an intense focus on cybersecurity. The policy has evolved from baseline definitions and sector identifications all the way to the current National Cybersecurity Framework for CI Protection and the National Infrastructure Protection Plan. Some national policies are classified documents authorizing cyber defenses that cannot be publicly detailed, and other policies are open source documents crafted with the inclusion of the public sector in mind. No single repository is available to which someone can refer, read, and understand U.S. cyber policy. In addition, no designated authority responsible for the overall mission of national cyber security and defense exists.

Other nations have taken different policy approaches to national cyber security policy on CI protection. The Australian government published

complimentary documents in back to back years to focus private and government sector stakeholders within this mission space. In 2009, Attorney General Robert McClelland published the Australian national "Cyber Security Strategy" to synergize efforts on national objectives to protect the Australian government, and business and civilian sectors from cyber threats. The document also specifically addresses ICS security[372] and CI cyber protection.[373]

In 2010, Attorney General Robert McClelland published the complimentary Australian national "Critical Infrastructure Resilience Strategy," which details an all hazards approach to national CI resiliency with an emphasis on cyber threats. The document outlines policy objectives within this mission space, with the Australian government's "Trusted Information Sharing Network" (TISN) noted as a focal point for government and private sector collaboration.[374] These two policy documents outline overarching frameworks Australians can utilize to understand the objectives, strategic priorities, and components of their national strategy. To achieve true national unity of effort in CI cyber security, a nation must first understand the strategic objectives to be accomplished in furtherance of that effort. These two documents provide that baseline understanding for Australians.

Defining the current policy of the United Kingdom, as it pertains to cyber security, is also a much simpler task than defining the U.S. policy. The United Kingdom publishes it's official policies under the "policies" tab of its official government website (https://www.gov.uk/government/policies).

A national policy document outlining a five-year strategy was published on November 25, 2011, and is entitled, "The UK Cyber Security Strategy: Protecting and Promoting the UK in a Digital World." The policy is introduced with a "written ministerial statement" from Francis Maude, the Minister for the Cabinet Office

372 Commonwealth of Australia, *Cyber Security Strategy*, 13.

373 Ibid., 20.

374 Commonwealth of Australia, *Critical Infrastructure Resilience Strategy* (Commonwealth of Australia: Attorney General's Department 2010), 17, http://www.emergency.qld.gov.au/publications/pdf/Critical_Infrastructure_Resilience_Strategy.pdf.

and Paymaster General. The statement notes that the U.K.'s National Security Strategy includes cybersecurity as one of the top tier national priorities and commits the equivalent of one billion U.S. dollars, over a five-year period, to develop the U.K. cyber response effort.[375]

The comprehensive policy document contains an ambitious vision for the end of that five-year time frame, that the measures outlined in the policy will put the United Kingdom in a position in which "law enforcement is tackling cyber criminals; citizens know what to do to protect themselves; effective cyber security is seen as a positive for U.K. business; a thriving cyber security sector has been established; public services online are secure and resilient; and threats to our national infrastructure and national security have been confronted."[376]

The policy breaks down specific action items underneath these overarching policy objectives. The policy candidly acknowledges the impossibility of absolute network security, and therefore, embraces a risk-based approach of prioritized response.[377] The ownership of most CI is recognized as privately owned, and the policy lays out the necessity for cooperation between individuals, the private sector, and the government. The policy pledges transparently and a commitment to report back on its progress.[378]

The U.K. Cyber Security Strategy has kept its promise of accountability and transparency by issuing progress report updates in December of each successive year. Updates are published by the U.K. Cabinet Office, which is identified as being responsible for overall national cyber security. Progress is tracked according to the specific action items listed in the policy's objectives. Impressive progress is noted in the December 2014 report, with many initiatives

---

[375] Cabinet Office and Paymaster General*, The UK Cyber Security Strategy—Protecting and Promoting the UK in a Digital World* (London: Cabinet Office and Paymaster General, 2011), 5, https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/60961/uk-cyber-security-strategy-final.pdf.

[376] Ibid.

[377] Ibid., 22.

[378] Ibid.

noted as performing well above predicted thresholds. It is another example of a government policy that promotes national unity of effort. The U.K. approach of publishing annual progress reports measures progress toward its five-year policy objective benchmarks and spotlights annual focus on the topic of CI cyber security to keep it at the forefront of the national conscience.

- Policy recommendation #1 is the creation of a new federal Department of Cyber Affairs, led by a presidential cabinet level Secretary of Cyber Affairs, and the subsequent assignment to the department of developing a unified cyber security policy for the United States.

A definitive document outlining an official cyber protection policy for the United States would promote national unity of effort for the military, business, and private sectors of the country. Target benchmarks could be established for strategic objectives and an annual progress report could measure progress and keep the discourse on this critical topic relevant nationally each year. A unified policy would currently require collaboration by the DOD for military operations, the DHS for domestic operations, and the Department of Justice for criminal investigations. It would be a tall task merging these bifurcated missions into one policy without leadership from a designated government official responsible for the overall cyber security of the United States.

Federal department heads are responsible for carrying out U.S. policy as directed by federal laws and presidential directives. Cyber security policy responsibility is currently diffused between several departments and does not have clear ownership. Comprehensive cyber security policy would be most effectively developed by a Department of Cyber Affairs, responsible specifically for that policy, with a Secretary who reported directly to the President as a member of his cabinet. This Secretary would in essence become the new focal point of cyber security for the nation and would be responsible for the development, coordination, and execution of overall cyber security policy to meet national objectives, such as protecting U.S. CIs. A definitive policy document outlining an official cyber security policy for the United States would promote

national unity of effort for the government, military, business, and private sectors. The newly appointed Secretary of Cyber Affairs would have implementation responsibility for the following two policy recommendations as well.

2. Expansion of Cyber Security Coordination between the Private and Government Sectors

Many of the activities that form the foundation of day-to-day life for American citizens and the government rely on potentially vulnerable networked computer systems. Networked computers are a critical component in most of the nation's 16 CI sectors. It is true as it pertains to military defense, public safety service delivery, the delivery of electricity, the transportation of people and goods, the banking industry, the communications industry, and the delivery of clean water. Interruptions to these, or other critical services, could be either disruptive or devastating for the nation's well-being and security.

Accordingly, cyber security for national CI ranks among the highest national security priorities. However, as noted earlier, the majority of U.S. CI remains under private management and control. The private ownership piece makes unifying CI cybersecurity particularly challenging because owners and managers set their own business priorities and determine their own cyber security defense measures.

Australia has chosen a consolidated cyber security approach that undertook its latest evolution in November 2014, with the opening of the Australian Cyber Security Centre (ACSC).[379] The ACSC condenses national cyber security capabilities, from across the government spectrum, into one location that serves as a hub for private and public sector collaboration to counter serious cyber threats.[380]

---

379 "Australian Cyber Security Centre," accessed November 8, 2015, http://www.asd.gov.au/infosec/acsc.htm.

380 Commonwealth of Australia, *2015 Threat Report* (Commonwealth of Australia: Australian Cyber Security Centre, 2015), 3, https://acsc.gov.au/publications/ACSC_Threat_Report_2015.pdf.

Six key Australian government agencies are co-located in a special purpose, high security building in Canberra, Australia.[381] All six partners provide expertise specific to their agencies to round out a protective posture for Australia's cyber assets. The Australian Signals Directorate furnishes expertise in information security and offers advice to government agencies. The Cyber Emergency Response Team (CERT Australia) serves as the anchor point of contact for major Australian businesses. The Australian Federal Police respond to and investigate cyber crimes of national significance. The Australian Crime Commission uncovers, analyzes, and prioritizes cyber threat intelligence information to support response options. The Australian Security Intelligence Organization provides cyber investigators and telecommunication security specialists. Finally, the Defense Intelligence Organization contributes strategic intelligence analysts.[382]

The United Kingdom took this concept of government agency collaboration a step further by establishing its Cybersecurity Information Sharing Partnership (CISP) in March 2013. CISP provides a collaborative platform for companies to share real time cyber threat information. A fusion center hub, comprised of private and government sector cybersecurity experts, examines the data and distributes enhanced intelligence and mitigation advice to the CISP membership. As of December 2014, CISP had 750 member organizations participating in the program.[383]

- Policy recommendation #2 is the consolidation of U.S. government cyber security expertise and assets for a more focused approach toward unified cyber defense for U.S. CIs.

U.S. national cyber security could benefit from the experiences of the United Kingdom and Australia, as it pertains to the bringing together of both

---

[381] "The Ben Chiefly Building," accessed November 8, 2015, http://www.asio.gov.au/About-ASIO/Ben-Chifley-Building.html.

[382] "Australian Cyber Security Centre."

[383] Cabinet Office and Paymaster General*, The UK Cyber Security Strategy—Protecting and Promoting the UK in a Digital World*, 5.

government and private sector expertise and assets to benefit national CI cyber security defenses. This second recommendation would pair neatly with the first recommendation of this thesis, which was the publishing of a unified cyber security policy by a newly appointed Secretary of Cyber Affairs.

Currently, U.S. CYBERCOM, U.S. military branches, U.S. intelligence agencies, the Department of Justice and the DHS field separately located cyber commands to focus in on their specific responsibilities pertaining to cyber security. These agencies could jointly house their experts under the umbrella of a new Department of Cyber Affairs to magnify the benefits of the expertise they have individually developed and reduce the potential for duplication of effort in a manner similar to the Australian Cyber Security Centre.

Among the agencies to be included within this consolidation would be U.S. CERT, which already analyzes U.S. cyber threats and communicates related information with trusted public sector and worldwide partners. The role of U.S. CERT could be expanded to include a U.K. CISP style fusion center composed of both government agency representatives and CI cyber security experts from the private sector. The collective expertise of a co-located cyber security fusion center would strengthen the defense of all 16 CI sectors. An additional benefit would be further buy-in from and encouragement of the private sector to engage actively in the cyber defense of U.S. privately owned CIs.

3. Incentivizing Private Sector Compliance with Best Practices in Cyber Security

It does not matter whether the U.S. military, U.S. government or a private sector entity operates a CI computer system; they are all potentially vulnerable to cyber attacks. Mandating best practice compliance measures from military or government held CIs is fairly simple and straightforward. However, privately controlled CIs pose a special challenge. Such companies operate under a traditional business model in which operational decisions will be made based on which option provides the best outlook for increased profits. Compelling private

sector companies to improve cybersecurity may carry a substantial price tag that could affect their short- or long-term profits. Some organizations believe that since the United States has not suffered a prominent cyber disruption of control systems, spending the time and money to update security for ICS prematurely, even if currently viewed as vulnerable to cyber attacks, is not economically justifiable when their current systems were designed to have 20+ year lifespans.[384]

Some potential solutions to coordinating the nation's cyber defenses of U.S. CIs are viewed unfavorably. Mandating business compliance with strict cyber security standards is viewed by many within industry as over-regulative, profit draining, and even dis-incentivizing of innovation in cyber defense practices and products that could ultimately benefit all sectors. Another potential solution would be allowing USCYBERCOM increased authority and responsibility over private sector CI protection. While potentially justifiable due to the disruptive and devastating effects a CI cyber attack could have on national well-being and security, it is another potential solution with considerable downside. Some believe it would be overly intrusive, could begin the "militarization of cyberspace," and could create distrust among cyber business and consumer markets.[385] Either of these mandated solutions would likely meet with stiff public sector resistance.

The United Kingdom has adopted a unique approach to gaining voluntary cyber security best practice compliance from its business sector. The most interesting aspect of the program is that it incentivizes businesses to want to come into best practice compliance because it offers them a competitive advantage in the marketplace, which speaks directly to businesses in a language they fully understand. The United Kingdom implemented its voluntary "Cyber Essentials" program in 2014 to reward cyber security best practices among

[384] Boaru and Badita, "Critical Infrastructure Protection Challenges and Efforts to Secure Control Systems," 157.

[385] Theohary and Harrington*. Cyber Operations in DOD Policy and Plans: Issues for Congress*, 27.

businesses. This government backed and industry supported program incentivizes widespread adoption of cyber security best practices that protect organizations against cyber attacks and gives them the ability to differentiate themselves in the marketplace for customers, investors, and business partners. Successful program certification of compliant businesses rewards them with a "badge" that firms can use to demonstrate their cyber security credentials publicly.[386]

The program provides businesses with guidance on implementing essential security controls to secure their networks better from most common cyber threats. Companies can apply for two levels of "badges" based on the level of rigor they want or need to demonstrate. "Cyber Essentials" badging requires the completion of a self-assessment questionnaire independently reviewed by a certifying body. "Cyber Essentials Plus" requires actual systems testing by an external certifying body. Once earned, certification badges provide companies with a marketing credential certifying to customers, partners, or clients that their company takes cyber security seriously. It bolsters the company's public reputation and provides a competitive selling point that can be leveraged in the marketplace.[387]

The resulting dynamic of this program is the creation of a profit driven business incentive that encourages the adoption of cyber security best practices. It benefits the resilience of the business community, U.K. CIs and the nation as a whole. The U.K. government further incentivized the program by requiring government contracts to be awarded to companies that have completed badging certification.[388] During the first six months of implementation, between June and December 2014, 124 companies were awarded the cyber essentials badge and

---

[386] Cabinet Office and Paymaster General*, The UK Cyber Security Strategy—Protecting and Promoting the UK in a Digital World*, 7.

[387] "Cyber Essentials," last viewed November 11, 2015, https://www.cyberstreetwise.com/cyberessentials/.

[388] Ibid.

30,000 more had viewed the web summary documents signifying significant interest.[389]

- Policy recommendation #3 is the development of a voluntary business cyber security certification program that allows businesses exhibiting cyber security best practices to be recognized in the marketplace for their commitment by customers, investors, and partners similar to the U.K.'s "Cyber Essentials" program.

The ability to incentivize cyber security best practices for U.S. businesses and CIs, by having these organizations view such a program as a marketplace advantage, would be a powerful tool in gaining voluntary compliance. The objective would be to create a competitive atmosphere in which companies would want to earn their certifications to assure customers of their cyber security prowess, to outpace competitors who may be slow to adopt best practices, and to develop a reputation as a cyber trustworthy company among their business partners.

The program could be structured in such a way as to feature tiered compliance levels of certification to address the differing needs of the business and CI community. The added incentive of requiring certification by companies seeking government contracts would further encourage many companies involved with securing CIs to make an effort to comply with best practices. Program development should take place as a shared venture with the business sector to ensure buy in and input from the ground level. The critical component of this program is ensuring it is something the business sector sees value in and wants to pursue for business reasons. This third policy recommendation could be implemented in conjunction with the first two recommendations and could fall under the purview of a newly created Department of Cyber Affairs.

[389] Cabinet Office and Paymaster General*, The UK Cyber Security Strategy—Protecting and Promoting the UK in a Digital World*, 7.

E. CONCLUSION

The objective of this thesis is to identify the pivotal areas of U.S. CI cyber protection policy that could be enhanced to provide the most effective overarching solutions to the current vulnerabilities highlighted by the Stuxnet attack on Iran, and provide subsequent recommendations for policy improvements. The three key areas in need of policy enhancement to bolster U.S. national CI and ICS defenses were identified as enhancing national unity of effort, expansion of coordination of effort between the private and government sectors, and incentivizing private sector compliance with best practices in cyber security.

The three overarching policy recommendations were identified as the following.

- The creation of a new federal Department of Cyber Affairs, led by a presidential cabinet level Secretary of Cyber Affairs, and the subsequent assignment to the department of developing a unified cyber security policy for the United States.
- The consolidation of U.S. government cyber security expertise and assets for a more focused approach toward unified cyber defense for U.S. CIs.
- The development of a voluntary business cyber security certification program that allows businesses exhibiting cyber security best practices to be recognized in the marketplace for their commitment by customers, investors and partners similar to the U.K.'s "Cyber Essentials" program.

These recommendations could be combined together as programs managed under a new federal Department of Cyber Affairs. They could potentially be implemented independently and managed by separate government entities that could be assigned responsibility for the initiatives. The downside to that approach would be the continued fragmentation of cyber security responsibility among stakeholders within the United States when unity of effort should be the key to this diverse landscape of military, government, business, and private sectors owners of U.S. CI.

The question then remains how will these policy recommendations prevent the United States from becoming the next victim nation of a Stuxnet style cyber attack? Three critical points of failure at Natanz enabled the attack. The critical points include system access, system security, and policy. These three crucial points all contributed to the failures that allowed Stuxnet to infiltrate, thrive within, and destroy centrifuges at Natanz.

The first point of failure at Natanz, leading to the Stuxnet infection, was the insider threat of system access at the facility. Stuxnet was engineered to be hand carried into the Natanz plant to infect the computer network. Symantec experts believe, "this may have occurred by infecting a willing or unknowing third party, such as a contractor who perhaps had access to the facility, or an insider."[390] The fact remains that negligent insiders spawn potential network access portals for malicious outsiders and incubate potential vulnerability for CIs in the United States.

The second point of failure at Natanz was the spread of Stuxnet through an air-gapped network to the PLCs, which controlled the precise spinning speed needed for proper centrifuge operations. Isolated and air gapped systems, such as the one at Natanz, have limited options when it comes to moving data between physically separated network computer systems.[391] Stuxnet was programmed to copy itself onto inserted removable drives, each time one was used, as one of its primary propagation methods. Thus, each time an infected removable drive was used to move data or instructions from one computer to another, the Stuxnet worm was also implanted.

These first two points of failure, system access and system security, fall into line with the third point of failure, which is policy. Although the Iranian government will not publicly share its Natanz policy portfolio, a deficiency exists in either establishing or following appropriate security protocols that led to the

[390] Falliere, Murchu and Chen, "W32.Stuxnet Dossier," 3.

[391] Niblick, "Protecting Critical Infrastructure against the Next Stuxnet," 19.

system access and system security breakdowns noted as the first two points of failure. Policy recommendations are the focus of the conclusion of this thesis.

The unfortunate reality is that no fail-safe set of countermeasures or policies is available that will provide complete immunity from CI cyber attacks. Cyber threats are evolving at a faster rate than the countermeasures employed to prevent them. Therefore, policy approaches must be vulnerability-based rather than threat-based. By focusing on reducing vulnerability, exposure is narrowed to all potential cyber threat vectors.[392]

The exposed Natanz vulnerabilities of the insider access threat, the transfer of data within a closed CI computer system on removable drives, and the policies supporting these functions, can all be addressed. Policy and procedure related to insider access can be effectively written, communicated, and enforced to limit system and sensitive data access to the smallest number of authorized users possible.[393] The objective is to restrict access as tightly as possible, while still allowing for efficient business operations, to narrow the insider threat vector as much as possible.

Stuxnet's propagation through the Natanz computer systems could also have been affected from a technology security policy standpoint. Policy restrictions on the use of portable media and drives, along with the encryption of sensitive system data, could have greatly reduced the vulnerability at Natanz had such restrictions been followed.[394] Data could still be securely moved through air-gapped CI systems like Natanz on removable storage drives with specific removable drive security software backed up by policies specifying which devices can be used and by whom. These are just the known vulnerabilities exposed by the Stuxnet attack. Other vulnerabilities may have been present but were not exploited.

---

[392] Crouch and McKee Jr., "Cybersecurity: What Have We Learned?," 2.

[393] Niblick, "Protecting Critical Infrastructure against the Next Stuxnet," 21.

[394] Ibid., 18.

Mandating policy reform can be one approach that would be effective perhaps for military or government controlled CIs. Policies and procedures can be published and enforced within these environments. Violations can be uncovered during audits and corrective measures can be administered when non-compliance is found. However, with most of the U.S. CI network falling under the control of private business, mandating policy measures for procedures or security upgrades is a challenge. Currently, no mechanism exists for mandating security procedures for most of the business sector.

The recommendations of this thesis start with unification of effort under a single national policy on cyber protection for U.S. CIs through a new federal department charged with cyber security for the nation. Under the umbrella of this new policy and department, a consolidation of currently fragmented cyber security expertise could occur so the nation's best and brightest minds in this field could work together jointly, regardless of agency assignment, to develop the most innovative cyber security solutions to the nation's most daunting threats. A voluntary but incentivized cyber security certification and credentialing program could be developed in partnership with business sector stakeholders. The objective would be to create a competitive atmosphere in which companies would want to earn cyber security certifications to assure customers of their cyber security prowess, to outpace competitors who may be slow to adopt best practices and to develop reputations as cyber trustworthy companies among business partners.

F. FUTURE RESEARCH OPPORTUNITIES

An important implication of the Stuxnet attack, but one outside the scope of this thesis, focuses on the education and skill sets of the people employed to protect U.S. CIs from cyber attacks. Rapid technical innovations and advancements in computer technology within U.S. CIs require the services of an increasingly technologically astute workforce. U.S. educational institutions are struggling to meet the growing demand for cyber security professionals in the

workforce, which has resulted in a gap that has left many cyber security jobs unfilled.[395] Questions for future consideration include the following.

- Are U.S. primary education system's curricula sufficiently educating children in the cornerstone cyber security educational fields of STEM to make them successful at the university level?
- Is the U.S. secondary education system appropriately postured, with the right programs at its universities, to educate the talent needed to fill jobs within the domestic cyber security workforce?
- Do non-traditional fields or vocations exist from which cyber security talent should be recruited?
- Are adequate internships and professional development programs available within the cyber security professional field of the United States to advance and train new employees entering the workforce?

The U.S. capacity to maintain it's standing as a technology innovator is key to its ability to protect U.S. CIs and their computerized ICS from future attacks. Education is and always will be the key to building a solid foundation for U.S. cyber defenses. Enough ground can be covered, and enough questions answered, on the educational side of cyber defense to satisfy several theses.

[395] Kay, Pudas, and Young, "Preparing the Pipeline: The U.S. Cyber Workforce for the Future," 1–2.

LIST OF REFERENCES

Abouzakhar, Nasser. “Critical Infrastructure Cybersecurity: A Review of Recent Threats and Violations.” *University of Hertfordshire School of Computer Science, Academic Conferences International Limited*, 2013. http://search.proquest.com/docview/1400694816?accountid=12702.

Agarwal, Tarun. “A Glance on Industrial Control Systems with Control Strategies.” EDGEFX.US, August 26, 2014. http://www.efxkits.us/industrial-control-systems-and-control-strategies/.

Arquilla, John. “Twenty Years of Cyberwar.” In *Military Ethics and Emerging Technologies,* edited by Timothy J. Demy, George R. Lucas Jr., and Bradley J. Strawser. London and New York: Routledge, 2014.

Australia Security Intelligence Organization. “The Ben Chiefly Building.” Accessed November 8, 2015. http://www.asio.gov.au/About-ASIO/Ben-Chifley-Building.html.

Barrett, Edward T. “Warfare in a New Domain: Ethics of Military Cyber-Operations.” In *Military Ethics and Emerging Technologies,* edited by Timothy J. Demy, George R. Lucas Jr., and Bradley J. Strawser. London and New York: Routledge, 2014.

BBC News. “Iran Profile—Timeline.” July 14, 2015. http://www.bbc.com/news/world-middle-east-14542438.

Boaru, Gheorghe, and George-Ionut Badita. “Critical Infrastructure Protection Challenges and Efforts to Secure Control Systems.” Romanian National Defense University, Regional Department of Defense Resources Management Studies, 2008. http://search.proquest.com/docview/1136853092?accountid=12702.

Cabinet Office, and Paymaster General. *The UK Cyber Security Strategy—Protecting and Promoting the UK in a Digital World*. London: Cabinet Office and Paymaster General, 2011. https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/60961/uk-cyber-security-

Cole, Eric. “Insider Threats and the Need for Fast and Directed Response.” SANS Institute, April 2015. https://www.sans.org/reading-room.

Commonwealth of Australia. *2015 Threat Report.* Commonwealth of Australia: Australian Cyber Security Centre 2015. https://acsc.gov.au/publications/ACSC_Threat_Report_2015.pdf.

———. “Australian Cyber Security Centre.” Accessed November 8, 2105. http://www.asd.gov.au/infosec/acsc.htm.

———. *Critical Infrastructure Resilience Strategy.* Commonwealth of Australia: Attorney General’s Department 2010. http://www.emergency.qld.gov.au/publications/pdf/Critical_Infrastructure_Resilience_Strategy.pdf.

———. *Cyber Security Strategy.* Commonwealth of Australia: Attorney General’s Department, 2009. https://www.ag.gov.au/RightsAndProtections/CyberSecurity/Documents/AG%20Cyber%20Security%20Strategy%20-%20for%20website.pdf.

Crouch, Jim E., and Larry K. McKee Jr. “Cybersecurity: What Have We Learned?.” National Security Cyberspace Institute, October 9, 2011. http://www.nsci-va.org/WhitePapers/2011-10-09-Cyber%20Lessons%20Learned-Crouch-McKee.pdf.

CSIS Strategic Technologies Program. “Cyber Incident Timeline.” July 29, 2015. http://www.csistech.org/cyber-incident-timeline/.

Davis, Michael A. “Stuxnet Reality Check: Are You Prepared for a Similar Attack?” Information Week Analytics in conjunction with Security Dark Reading, May 2011. http://i.techweb.com/darkreading/advancedthreat/S2840511_DR_stuxnet.pdf.

Denning, Dorothy E. “Framework and Principles for Active Cyber Defense.” Essay, Naval Postgraduate School, 2013. http://faculty.nps.edu/dedennin/publications/Framework%20and%20Principles%20for%20Active%20Cyber%20Defense%20-%2011Dec2013.pdf.

Dodaro, Gene L. *Report to Congressional Committees: High-Risk Series, an Update*. (GAO-15-290). Washington, DC: U.S. Government Accountability Office, 2015. http://www.gao.gov/assets/670/668415.pdf.

Drogin, Bob. “Russians Seem to be Hacking into Pentagon.” *Los Angeles Times*, October 7, 1999. http://www.sfgate.com/news/article/Russians-Seem-To-Be-Hacking-Into-Pentagon-2903309.php.

Ernst, Aaron. “Is this the Future of Cyberwarfare?.” AlJazeera America, February, 5, 2015. http://america.aljazeera.com/watch/shows/america-tonight/articles/2015/2/5/blackenergy-malware-cyberwarfare.html.

Etzioni, Amitai. “The Private Sector: A Reluctant Partner in Cybersecurity.” The George Washington University, December 19, 2014. https://icps.gwu.edu/private-sector-reluctant-partner-cybersecurity.

Executive Office of the President of the United States. *The Comprehensive National Cybersecurity Initiative*. Washington, DC: Executive Office of the President of the United States, 2009.

Falliere, Nicolas, Liam Murchu and Eric Chen. “W32.Stuxnet Dossier.” Symantec, February 2011. https://www.symantec.com/content/en/us/enterprise/media/security_response/whitepapers/w32_stuxnet_dossier.pdf.

Finkle, Jim. “Factbox: Cyber Warfare Expert’s Timeline for Iran Attack.” Reuters, December 2, 2011. http://www.reuters.com/article/2011/12/02/us-cyberattack-iran-idUSTRE7B10AV20111202.

———. “Researchers Say Stuxnet Was Deployed against Iran in 2007.” *Reuters*, February 26, 2013. http://www.reuters.com/article/2013/02/26/us-cyberwar-stuxnet-idUSBRE91P0PP20130226.

Flowers, Angelyn, and Sherali Zeadally. “U.S. Policy on Active Cyber Defense.” *Journal of Homeland Security and Emergency Management* 11, no. 2 (2014): 289–308. doi:http://dx.doi.org/10.1515/jhsem-2014-0021.

Glenny, Misha, and Camino Kavanagh. “800 Titles but no Policy—Thoughts on Cyber Warfare.” *American Foreign Policy Interests* 34, no. 6 (2012): 287–294. http://search.proquest.com.libproxy.nps.edu/docview/1264925856?accountid=12702.

Henrie, Morgan. “Cyber Security Risk Management in the SCADA Critical Infrastructure Environment.” *Engineering Management Journal* 25, no. 2 (June 2013): 38–45. http://search.proquest.com/docview/1434438191?accountid=12702.

Herzog, Stephen. “Revisiting the Estonian Cyber Attacks: Digital Threats and Multinational Responses.” *Journal of Strategic Security* 4, no. 2 (Summer 2011): 49–60. http://scholarcommons.usf.edu/cgi/viewcontent.cgi?article=1105&context=jss.

HM Government—The Home Office. “Cyber Essentials.” Last viewed November 11, 2015. https://www.cyberstreetwise.com/cyberessentials/.

Hosenball, Mark. “Experts Say Iran Has Neutralized Stuxnet Virus.” *Reuters*, February 14, 2012. http://www.reuters.com/article/2012/02/14/us-iran-usa-stuxnet-idUSTRE81D24Q20120214.

ICS-CERT. “About the Industrial Control System Cyber Emergency Response Team.” Accessed October 24, 2015. https://ics-cert.us-cert.gov/About-Industrial-Control-Systems-Cyber-Emergency-Response-Team.

Jenkins, Ryan. “Is Stuxnet Physical? Does it Matter?.” In *Military Ethics and Emerging Technologies,* edited by Timothy J. Demy, George R. Lucas Jr., and Bradley J. Strawser, 263–264. London and New York: Routledge, 2014.

Karnouskos, Stamatis. “Stuxnet Worm Impact on Industrial Cyber-Physical System Security.” Paper presented at the 37th Annual Conference of the IEEE Industrial Electronics Society (IECON 2011), Melbourne, Australia, November 7–10, 2011. http://papers.duckdns.org/files/2011_IECON_ stuxnet.pdf.

Kay, David J., Terry J. Pudas, and Brett Young. “Preparing the Pipeline: The U.S. Cyber Workforce for the Future.” *Defense Horizons,* no. 72 (August 2012): 1–16. http://search.proquest.com/docview/1038377323?accountid=127 02.

Kelley, Michael. “The Stuxnet Attack on Iran’s Nuclear Plant Was ‘Far More Dangerous’ Than Previously Thought.” *Business Insider*, November 20, 2013. http://www.businessinsider.com/stuxnet-was-far-more-dangerous-than-previous-thought-2013-11.

Kerr, Paul K. *Iran’s Nuclear Program: Tehran’s Compliance with International Obligations* (CRS Report No. R40094). Washington, DC: Congressional Research Service, 2015. http://fas.org/sgp/crs/nuke/R40094.pdf.

Kerr, Paul K. John Rollins, and Catherine A. Theohary. *The Stuxnet Computer Worm: Harbinger of an Emerging Warfare Capability* (CRS Report No. R41524). Washington, DC: Congressional Research Service, 2010. http://www.fas.org/sgp/crs/natsec/R41524.pdf.

Khandelwal, Swati. “Stuxnet-like ‘Havex’ Malware Strikes European SCADA Systems.” The Hacker News, June 26, 2014. http://thehackernews.com/ 2014/06/stuxnet-like-havex-malware-strikes.html.

Kroft, Steve. “Stuxnet: Computer Worm Opens New Era of Warfare.” CBS News, June 1, 2012. http://www.cbsnews.com/news/stuxnet-computer-worm-opens-new-era-of-warfare-04-06-2012/.

Kushner, David. “The Real Story of Stuxnet.” *IEEE Spectrum*, February 1, 2013. http://spectrum.ieee.org/telecom/security/the-real-story-of-stuxnet.

Langer, Ralph. “To Kill a Centrifuge.” The Langer Group, November 2013. http://www.langner.com/en/wp-content/uploads/2013/11/To-kill-a-centrifuge.pdf.

Lynn, William J. III. “Defending a New Domain.” *Foreign Affairs*. Accessed November 29, 2015. https://www.foreignaffairs.com/articles/united-states/2010-09-01/defending-new-domain.

McLachlan, Keith S. “Iran in 2006.” *Encyclopedia Britannica*. Accessed September 19, 2015. http://www.britannica.com/place/Iran-Year-In-Review-2006.

MENA Report. “United States: Unisys Survey Reveals Nearly 70 Percent of Critical Infrastructure Providers Have Been Breached in the Past Year.” July 11, 2014. http://search.proquest.com/docview/1544450370?accountid=12702.

Mitchell, Bradley. “Computer Worm—Internet Security Terms.” Accessed February 3, 2015. *Compnetworking*. http://compnetworking.about.com/cs/worldwideweb/g/bldef_worm.htm.

Moteff, John D. *Critical Infrastructures: Background, Policy, and Implementation* (CRS Report No. RL30153). Washington, DC: Congressional Research Service, 2015. http://fas.org/sgp/crs/homesec/RL30153.pdf.

Nakashima, Ellen “Hacks of OPM Databases Compromised 22.1 Million People, Federal Authorities Say.” *Washington Post*, July 9, 2015. https://www.washingtonpost.com/news/federal-eye/wp/2015/07/09/hack-of-security-clearance-system-affected-21-5-million-people-federal-authorities-say/.

———. “Obama Signs Secret Directive to Help Thwart Cyberattacks.” *Washington Post*, November 14, 2012. https://www.washingtonpost.com/world/national-security/obama-signs-secret-cybersecurity-directive-allowing-more-aggressive-military-role/2012/11/14/7bf51512-2cde-11e2-9ac2-1c61452669c3_story.html.

———. “Stuxnet Malware Is Blueprint for Computer Attacks on U.S..” *Washington Post*, October 2, 2010. http://www.washingtonpost.com/wp-dyn/content/article/2010/10/01/AR2010100106981.html?sid=ST2010112903583.

National Institute of Standards and Technology. *Framework for Improving Critical Infrastructure Cyber Security*. Gaithersburg, MD: National Institute of Standards and Technology, 2014.

NetDiligence. “2015 Cyber Claims Study.” September 2015. http://netdiligence.com/articles.php.

News 24. “Cyber Terror Targets Utilities.” May 31, 2012. http://www.news24.com/SciTech/News/Cyber-terror-targets-utilities-20120531.

Niblick, Doug. “Protecting Critical Infrastructure against the Next Stuxnet.” Davenport University, March 20, 2013. http://www.davenport.edu/system/files/Protecting_Critical_Infrastructure_Against_the_Next_Stuxnet.pdf.

Paletta, Damian, Danny Yadron, and Jennifer Valentino-DeVries. “Cyberwar Ignites New Arms Race.” *Wall Street Journal*, October 12, 2015. http://www.wsj.com/articles/cyberwar-ignites-a-new-arms-race-1444611128.

Pctools. “What is a Zero Day Vulnerability?.” Symantec. Accessed September 19, 2015. http://www.pctools.com/security-news/zero-day-vulnerability/.

Rinaldi, Steven M., James P. Peerenboom, and Terrence K. Kelly. “Identifying, Understanding, and Analyzing Critical Infrastructure Interdependencies.” *IEEE Control Systems Magazine*. December 2001. http://user.it.uu.se/~bc/Art.pdf.

Rouse, Margaret. “Worm Definition.” Tech Target Network. Last accessed November 29, 2015. http://searchsecurity.techtarget.com/definition/worm.

Sanger, David. “Obama Order Sped Up Wave of Cyberattacks Against Iran.” *New York Times*, May 31, 2012. http://www.nytimes.com/2012/06/01/world/middleeast/obama-ordered-wave-of-cyberattacks-against-iran.html?pagewanted=all&_r=0.

Setalvad, Ariha. “Demand to Fill Cybersecurity Jobs Booming.” Peninsula Press of Stanford, March 31, 2015. http://peninsulapress.com/2015/03/31/cybersecurity-jobs-growth/.

Sharafedin, Bozorgmehr. “Why Iran Takes Issue with the Holocaust.” *BBC News*, October 9, 2013. http://www.bbc.com/news/world-middle-east-24442723.

Shea, Dana A. *Critical Infrastructure: Control Systems and the Terrorist Threat* (CRS Report No. RL31534). Washington, DC: Congressional Research Service, 2004. http://fas.org/irp/crs/RL31534.pdf.

Stouffer, Keith, Suzanne Lightman, Victoria Pillitteri, Marshall Abrams, and Adam Hahn. *Guide to Industrial Control Systems Security* (NIST-800-82). Gaithersburg, MD: National Institute of Standards and Technology, 2014. http://csrc.nist.gov/publications/nistpubs/800-82/SP800-82-final.pdf.

Tereshchenko, Natalia. “U.S. Foreign Policy Challenges of Non-State Actors’ Cyber Terrorism against Critical Infrastructure.” *International Journal of Cyber Warfare and Terrorism* 2, no. 4 (October 2012): 28–48. http://search.proquest.com/docview/1465900385?accountid=12702.

Theohary, Catherine A., and Anne I. Harrington. *Cyber Operations in DOD Policy and Plans: Issues for Congress* (CRS Report No. R43848). Washington, DC: Congressional Research Service, 2015. http://fas.org/sgp/crs/natsec/R43848.pdf.

U.S. Department of Homeland Security. “Industrial Control Systems Cyber Emergency Response Team.” accessed February 13, 2015. https://ics-cert.us-cert.gov/content/cyber-threat-source-descriptions.

———. “Chemical Sector.” Last modified July 16, 2015. http://www.dhs.gov/chemical-sector.

———. “Commercial Facilities Sector.” Last modified August 27, 2014. http://www.dhs.gov/chemical-sector.

———. “Critical Infrastructure Protection Partnerships and Information Sharing.” Last modified April 14, 2015. http://www.dhs.gov/critical-infrastructure-protection-partnerships-and-information-sharing.

———. “Critical Manufacturing Sector.” Last modified December 4, 2014. http://www.dhs.gov/critical-manufacturing-sector.

———. “Cybersecurity Overview.” Last modified September 22, 2015. http://www.dhs.gov/cybersecurity-overview.

———. “Dams Sector.” Last modified December 11, 2014. http://www.dhs.gov/dams-sector.

———. “Defense Industrial Base Sector.” Last modified June 12, 2014. http://www.dhs.gov/defense-industrial-base-sector.

———. “Energy Sector.” Last modified June 17, 2015. http://www.dhs.gov/energy-sector.

———. “Financial Services Sector.” Last modified June 12, 2014. http://www.dhs.gov/financial-services-sector.

———. “Food and Agriculture Sector.” Last modified June 12, 2014. http://www.dhs.gov/food-and-agriculture-sector.

———. “Government Facilities Sector.” Last modified June 12, 2014. http://www.dhs.gov/government-facilities-sector.

———. “Health and Public Health Sector.” Last modified June 12, 2014. http://www.dhs.gov/healthcare-and-public-health-sector.

———. “Information Technology Sector.” Last modified June 12, 2014. http://www.dhs.gov/information-technology-sector.

———. *NIPP 2013: Partnering for Critical Infrastructure Security and Resilience*. Washington, DC: U.S. Department of Homeland Security, 2013.

———. “Nuclear Reactors, Materials and Waste Sector.” Last modified November 24, 2014. http://www.dhs.gov/nuclear-reactors-materials-and-waste-sector.

U.S. Department of Homeland Security. “Protecting Critical Infrastructure.” September 23, 2015. http://www.dhs.gov/topic/protecting-critical-infrastructure.

———. “Transportation Systems Sector.” Last modified March 25, 2013. http://www.dhs.gov/transportation-systems-sector.

———. “Water and Wastewater Systems Sector.” Last modified June 12, 2014. http://www.dhs.gov/water-and-wastewater-systems-sector.

———. “What is Critical Infrastructure.” Last modified October 24, 2013. http://www.dhs.gov/what-critical-infrastructure.

U.S. Government Accountability Office. *Critical Infrastructure Protection—Progress Coordinating Government and Private Sector Efforts Varies by Sectors’ Characteristics*. (GAO-07-39). Washington, DC: U.S. Government Accountability Office, 2006. http://www.gao.gov/new.items/d0739.pdf.

U.S. Strategic Command. “U.S. Cyber Command.” March 2015. https://www.stratcom.mil/factsheets/2/Cyber_Command/.

Urrico, Roy. “Negating Cybersecurity Threats from Within.” *Credit Union Times*, June 3, 2015. http://search.proquest.com/docview/1685156530?accountid=12702.

Veltsos, Christophe. “Addressing the Information Security Skills Gap in Partnership with Academia.” Security Intelligence, October 9, 2015. https://securityintelligence.com/addressing-the-information-security-skills-gap-in-partnership-with-academia/.

Warrick, Joby. “Iran’s Natanz Nuclear Facility Recovered Quickly from Stuxnet Cyberattack.” *Washington Post*, February 16, 2011. http://www.washingtonpost.com/wp-dyn/content/article/2011/02/15/AR2011021505395.html.

White House Office of the Press Secretary, The. *Critical Infrastructure Protection*. Presidential Decision Directive 63. Washington, DC: The White House Office of the Press Secretary, 1998.

———. *Critical Infrastructure Security and Resilience*. Presidential Decision Directive 21. Washington, DC: The White House Office of the Press Secretary, 2013.

———. *Cyber Operations*. Presidential Decision Directive 20 (Fact Sheet Only), Washington, DC: The White House Office of the Press Secretary, 2013.

Wisegeek. "What Are Digital Certificates?" http://www.wisegeek.com/what-are-digital-certificates.htm.

———. "What Is a Programmable Logic Controller (PLC)?." June 20, 2015. http://www.wisegeek.org/what-is-a-programmable-logic-controller.htm.

Yonah, Jeremy. "U.S. Tries Policy of 'Shame' to Stem Chinese Cyber-Hacking." *Jerusalem Post,* August 17, 2014. http://search.proquest.com/docview/1555615443?accountid=12702.

THIS PAGE INTENTIONALLY LEFT BLANK

INITIAL DISTRIBUTION LIST

1. Defense Technical Information Center
   Ft. Belvoir, Virginia

2. Dudley Knox Library
   Naval Postgraduate School
   Monterey, California